

## 明 細 書

## 情報処理サーバ及び情報処理方法

## 技術分野

本発明は、いつでもどこでも情報通信を行える、いわゆる「ユビキタス」通信環境下において、個人情報を保護しながら電子商取引を行う技術に係り、特に認証情報を利用した情報処理方法、及びこの情報処理方法に用いる情報処理サーバに関する。更には、異機種間の通信端末での画像情報の通信の互換性等を実現するための技術に関する。

## 背景技術

現在、インターネットと携帯端末の普及によりいつでもどこでも情報通信を行えるようになってきている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられており、暗号化されたH T T P S

(Hypertext Transfer Protocol Security)などのプロトコルを利用して情報をサーバに送信することも頻繁に行われている。そのため通信される情報が他人に漏れないように様々な暗号化が考えられている。暗号化方式にも秘密鍵方式や公開鍵方式等が利用されている。発信者から受信者まで単純に情報が伝達される場合、発信者と受信者の間で暗号化鍵を決めておけば暗号を解読されな

い限りそれ程問題とはならない。しかし電子商取引等では、個人情報認証するサーバと実際に商取引を行うサーバが異なることがほとんどである。更にネットワークが複雑になり、種々の情報を同時にやり取りするようになると処理に係わるサーバの数は多くなる。したがって全情報を一括して暗号化してしまうと、途中のサーバで全情報を復号する必要が生じ、サーバに不必要な情報までもが知られてしまうことになる。この様に複数のサーバで処理される情報を、必要な部分のみ参照できるようにして情報を保護する方法はまだ考えられていない。

携帯端末の場合、規格が通信事業者によって決まるため、例えば、携帯端末を識別する機器識別子を取得することにより、サーバは携帯端末の認証を高い精度で行うことができるが、インターネット等の通信ネットワークにおいて、コンピュータ等の認証を行うことは困難とされている。即ち、コンピュータでインターネット等に接続するために利用するブラウザやHTTP（Hypertext Transfer Protocol）などのプロトコルによれば、携帯端末の様に、コンピュータを識別する識別子を取得しサーバに送信することが不可能である。実際は、ブラウザのクッキーにサーバが作成した暗号化された暗号文を記憶し、認証時にその暗号文をサーバに送信したり、サーバへの接続時にユーザにパスワードを入力させるなどの方法が一般的である。

特開 2003-6164 号公報に開示されているよ

うに、W e b 上の提携サイトとネットワークを介して接続され、提携サイトへのアクセスが許容されたユーザの認証情報を格納するユーザ情報データベースと、提携サイトへ入力された認証情報を取得し、ユーザ情報データベースに基づいて認証処理を行い、認証結果を提携サイトへ送信する制御手段（モジュール）とを備えた認証システムなどがある。

又、二次元コード読取機能付き通信端末が開発され、二次元コード画像化された情報を通信端末に取り込むことが可能となった。更に、一部の通信端末には、二次元コード生成機能が内蔵されている。これにより通信端末の画面上に、情報を二次元コード化した画像を表示し、その画像を他の通信端末で読み取ることにより、通信端末間で情報の受け渡しが可能となってきた（後藤祥子、“ZDNet/JAPAN”、[online]、2003年7月15日、[平成15年9月22日検索]、インターネット<URL ;  
[http://www.zdnet.co.jp/mobile/0307/15/n\\_qrprint.html](http://www.zdnet.co.jp/mobile/0307/15/n_qrprint.html)> 参照。）。

#### 発明の開示

ユビキタスコンピューティングでは、必ずしもパーソナルコンピュータや携帯電話を必要としない。一般的にユビキタスコンピューティングは、加入者識別手段（モジュール）（S I M）カード、I C チップ又は無線タグ

(RFID)等からなる自動認識タグとウェアラブルコンピュータと複数のサーバからなるメタサーバによって実現される。このような環境下では、セキュリティ及び個人情報の保護が非常に重要になってくる。特にウェアラブルコンピュータでは、第3者に絶対に知られたくない情報をユーザが持ち歩く可能性があるため、こうした個人情報を送信する際、第3者に知られることなく、安全に当事者間での情報の送受信が行われるシステムの実現が重要となってきた。しかしながら、ユビキタス環境下における次世代ウェアラブルコンピュータによる通信において、個人情報保護の技術について標準的な方法は存在しない。又、ウェアラブルコンピュータのメモリ領域に記憶される情報量も増加の傾向にあり、メモリ容量が不足するという問題があった。

しかし上述した特開2003-6164号公報に開示された発明においては、認証システムにおいてのみ認証されれば、複数の提携サイトについての認証は必要ないが、認証システムにおける認証において盗聴された場合、ユーザの損失は計り知れないものがある。

一方、携帯電話機などの携帯端末の普及に伴い、携帯電話を利用して様々なサービスを享受するユーザが多く、サービスの提供時には氏名、住所などの個人情報を登録する場合がある。この場合、入力するユーザインターフェースに乏しい携帯端末においてこれらの個人情報を登録するのは非常に困難であり、コンピュータでの登録を



望むユーザも多い。しかしコンピュータでの登録においては、上述したようなユーザ認証時の問題があり、これを打破するシステムの開発が望まれている。

情報の二次元コード化の記述方式が通信端末の機種によって異なるため、異機種間の通信端末では、画像を読み取れたとしてもデータ形式が崩れてしまう。したがって、通信端末の機能を十分に生かすためには、出力側と読取側が同機種でなければいけない。そのため、機種間の互換性を実現するシステムの開発が望まれている。

本発明は、ユビキタス環境下における次世代ウェアラブルコンピュータによる通信において、個人情報等のデータを当事者以外から秘匿しながら電子商取引を可能とする情報処理方法、及びこの情報処理方法に用いる情報処理サーバを提供することを目的とする。

上記目的を達成するため、本発明の第1の特徴は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバに関する。即ち、本発明の第1の特徴に係る情報処理サーバは、(a) 認証情報を記憶した認証情報記憶装置；(b) 通信端末の認証依頼を受信する；(c) 認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証

パラメータ記憶装置に記憶する認証画像生成モジュール；（d）通信端末から取得した認証画像の情報；（e）認証端末が備える認証情報を、認証端末から取得する認証情報取得モジュール；（f）認証パラメータ記憶装置を参照して、認証情報取得モジュールで取得した認証画像の情報が、認証画像生成モジュールで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報照合モジュールとを備えることを要旨とする。

本発明の第2の特徴は、認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法に関する。即ち、本発明の第2の特徴に係る情報処理方法は：

（a）認証情報を認証情報記憶装置に記憶するステップ；

（b）認証画像生成モジュールによって、通信端末の認証依頼を受信する；

（c）認証パラメータを生成し、認証パラメータを含む認証画像を生成して通信端末に送信し、認証パラメータを認証パラメータ記憶装置に記憶する認証画像を生成するステップ；

（d）認証情報取得モジュールによって、認証端末から、通信端末から取得した認証画像の情報；

(e) 認証端末が備える認証情報を取得するステップ

(f) 認証情報照合モジュールによって、認証パラメータ記憶装置を参照して、認証画像の情報が、認証画像を生成するステップで生成された画像の情報であり、更に、認証端末が備える認証情報が、認証情報記憶装置に記憶した認証情報と一致するか否かを判定し、その結果を通信端末に送信する認証情報を照合するステップとを含むことを要旨とする。

本発明の第3の特徴は、通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置と、通信端末から入力される情報を、対応情報に従って変換する情報変換モジュールとを備える情報処理サーバであることを要旨とする。

本発明の第4の特徴は、第1端末、第2端末、及び第1端末と第2端末間を仲介する情報処理サーバとを含むシステムを用いた情報処理方法に関する。即ち、本発明の第4の特徴に係る情報処理方法においては、情報処理サーバが：

(a) 第1端末からのアクション要求を、第1レベルの個人情報と共に受信し、

(b) 第1レベルの個人情報により、第1端末を認証し、

(c) 第 1 端末に認証情報を発行し、

(d) 第 1 レベルの個人情報よりもセキュリティレベルの高い第 2 レベルの個人情報を、認証情報と共に第 1 端末から受信し、

(e) 認証情報に基づき、アクションに第 2 レベルの個人情報を第 2 端末に送信する

ことを要旨とする。

#### 図面の簡単な説明

図 1 は、本発明の第 1 の実施例に係る情報処理システムを説明するデータフロー図である。

図 2 は、本発明の第 1 の実施例に係る情報保護方式における第 1 の暗号化鍵取得システムを説明するデータフロー図である。

図 3 は、本発明の第 1 の実施例に係る情報保護方式における第 2 の暗号化鍵取得システムを説明するデータフロー図である。

図 4 は、本発明の第 2 の実施例に係る電子商取引における情報処理システムを説明するデータフロー図である。

図 5 は、本発明の第 3 の実施例に係るコミュニティ内の情報交換における情報処理システムを説明するデータフロー図である。

図 6 は、本発明の第 4 の実施例に係る暗号化鍵取得システムを説明するデータフロー図である。

図 7 は、本発明の第 4 の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図 8 は、本発明の第 5 の実施例に係る暗号化鍵取得方法を示す模式図である。

図 9 は、本発明の第 5 の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図 10 は、本発明の第 6 の実施例に係る暗号化鍵取得方法を示す模式図である。

図 11 は、本発明の第 6 の実施例に係る暗号化鍵取得方法を示すフローチャートである。

図 12 は、本発明の第 7 の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図 13 は、本発明の第 7 の実施例に係る情報処理方法を示すシーケンス図である。

図 14 は、本発明の第 8 の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図 15 は、本発明の第 8 の実施例に係る情報処理方法を示すシーケンス図である。

図 16 は、本発明の第 8 の実施例の変形例に係る情報処理方法を示すシーケンス図である。

図 17 は、本発明の第 9 の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図 1 8 は、本発明の第 9 の実施例に係る情報処理サーバがユーザに提示する質問リストとそのセレクトリストの一例である。

図 1 9 は、関連技術のパスワードによる認証の場合の組合せを示した図である。

図 2 0 は、本発明の第 9 の実施例に係る情報処理方法を示すシーケンス図である。

図 2 1 は、本発明の第 1 0 の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図 2 2 は、本発明の第 1 0 の実施例に係る情報処理方法を示すシーケンス図である。

図 2 3 は、本発明の第 1 1 の実施例に係る情報処理サーバの機能ブロック図と、情報処理サーバが用いられる情報処理システムのシステム構成図である。

図 2 4 は、本発明の第 1 1 の実施例に係る通信許可時の情報処理方法を示すシーケンス図である。

図 2 5 は、本発明の第 1 1 の実施例に係る通信不許可時の情報処理方法を示すシーケンス図である。

図 2 6 は、本発明の第 1 2 の実施例に係る情報処理システムのシステム構成図である。

図 2 7 は、本発明の第 1 2 の実施例に係る情報処理方法を説明するフローチャートである。

図 2 8 は、本発明の第 1 2 の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートで

ある。

図 2 9 は、本発明の第 1 2 の実施例の変形例に係る情報処理方法を説明するフローチャートである。

図 3 0 は、本発明の第 1 2 の実施例の他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図 3 1 は、本発明の第 1 2 の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図 3 2 は、本発明の第 1 2 の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図 3 3 は、本発明の第 1 3 の実施例に係る情報処理システムのシステム構成図である。

図 3 4 は、本発明の第 1 3 の実施例に係る情報処理方法を説明するフローチャートである。

図 3 5 は、本発明の第 1 3 の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートである。

図 3 6 は、本発明の第 1 4 の実施例に係る情報処理システムのシステム構成図である。

図 3 7 は、本発明の第 1 4 の実施例に係る情報処理方法を説明するフローチャートである。

図 3 8 は、本発明の第 1 4 の実施例に係る情報処理方法における情報処理サーバに着目したフローチャートである。

図 3 9 は、本発明の第 1 4 の実施例の変形例に係る情報処理方法を説明するフローチャートである。

図 4 0 は、本発明の第 1 4 の実施例の他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

図 4 1 は、本発明の第 1 4 の実施例の更に他の変形例に係る情報処理方法の処理の流れを説明する模式図である。

#### 発明を実施するための最良の形態

次に、図面を参照して、本発明の第 1 乃至第 1 4 の実施例を説明する。以下の図面の記載において、同一又は類似の部分には同一又は類似の符号を付している。但し、図面は模式的なものであり、比率等は現実のものとは異なることに留意すべきである。したがって、具体的な構造は以下の説明を参酌して判断すべきものである。又図面相互間においても互いの寸法の関係や比率が異なる部分が含まれていることは勿論である。

#### (第 1 の実施例)

本発明の第 1 の実施例に係る個人情報保護方式について、図 1、図 2 及び図 3 を参照しながら説明する。図 1 で「 $E_n(X)$ 」で表現しているものは、第  $n$  サーバによって復号できるように暗号化鍵によって  $X$  というデータを暗号化して生成された情報を示している。例えば「 $E$



3 (DATA1)」は、第2サーバ74によって復号できるように暗号化鍵によってDATA1というデータを暗号化した情報となる。図1では例示的に $n=3$ として説明する。

まず、図1に示すユビキタスコンピューティングでは、ユーザが利用する第1のウェアラブルコンピュータとしての携帯情報端末10aと、第1のウェアラブルコンピュータ（携帯情報端末）10aから送信される送信元メタデータMD0を処理する複数のサーバからなるメタサーバ76と、データの送信先である送信先サーバR40が存在する。ここでメタサーバ76は、例示的に第1サーバ72、第2サーバ73、第2サーバ74、送信サーバ24のサーバ群と、各サーバを接続する第1の匿名通信路71a、第2の匿名通信路71b、第3の匿名通信路71cと、第2サーバ73に接続された暗号化情報データベース25から構成されているものとする。実際にはサーバ、通信路そしてデータベースの数には制限はない。「匿名通信路」とは、通信されるパケット情報が他人にのぞき見されないようにした通信路であり、LANケーブル接続通信路、無線接続通信路、専用線接続通信路等のいずれであっても良い。

図1を参照しながら、情報保護方法について説明する

(a) 第1のウェアラブルコンピュータ(携帯情報端末) 10aで、第1サーバ72によってのみ復号できる暗号化鍵で第1の情報DATA3を暗号化し第1の暗号化情報E1(DATA3)を生成し、第2サーバ73によってのみ復号できる暗号化鍵で第2の情報DATA2を暗号化し第2の暗号化情報E2(DATA2)を生成し、第2サーバ74によってのみ復号できる暗号化鍵で第3の情報DATA1を暗号化し第3の暗号化情報E3(DATA1)を生成し、メタサーバ76は送信元メタデータMD0として受信する。DATA1、DATA2、DATA3、……とは、例えば個人認証情報、端末情報、送信先情報、商品情報、メール情報、画像情報等の情報である。

(b) 送信元メタデータMD0を受信した第1サーバ72は、第1サーバ72で処理に必要なかつ復号できる情報を検出する。図1では、E1(DATA3)があるので、これを復号してDATA3を得て処理を行う。その後、DATA3を送信先サーバR40で復号できるように再度暗号化してER(DATA3)に置換する。そして第1送信メタデータMD1を生成し、第1の匿名通信路71aを経由して第2サーバ73に送信する。その他の情報は第1サーバ72では復号できないため、第1サーバ72に対しては秘匿されていることになる。なお、別のサーバで復号できるように暗号化するための暗号化鍵取得方法については、図2及び図3を参照しながら後

で詳述する。

(c) 第1送信メタデータMD1を受信した第2サーバ73は、第2サーバ73で処理に必要かつ復号できる情報を検出する。図1では、E2(DATA2)があるので、第1サーバ72で行った方法と同様にして復号してDATA2を得て処理を行う(図示せず)。その後、DATA2を送信先サーバR40で復号できるように再度暗号化してER(DATA2)に置換する。又、もう1つの処理として、第2サーバ73では復号化して情報の内容を知ることができない情報を利用して、新たな情報を追加する。図1では、E3(DATA1)は第2サーバ74で復号されるものであるが、第2サーバ73に接続された暗号化情報データベース25の内容をこのE3(DATA1)をキー情報として第n+1の暗号化情報E3(INFO2)を得る。そしてE3(INFO2)を追加して第2送信メタデータMD2を生成し、第2の匿名通信路71bを経由して第2サーバ74に送信する。

(d) 第2送信メタデータMD2を受信した第2サーバ74は、第2サーバ74で処理に必要かつ復号できる情報を検出する。図1では、E3(DATA1)とE3(INFO2)があるので、第1サーバ72で行った方法と同様にして復号してDATA1とINFO2を得て処理を行う。その後、DATA1とINFO2を送信先サーバR40で復号できるように再度暗号化してER(DATA1)とER(INFO2)に置換する。そし

て第3送信メタデータMD3を生成し、第3の匿名通信路71cを経由して送信サーバ24に送信する。

(e) 送信サーバ24は送信先アドレスによって、第3送信メタデータMD3をメタサーバ76外の送信先サーバR40に送信する。最終的な第3送信メタデータMD3内の情報は送信先サーバR40で復号できるように、経由してきた第1サーバ72、第2サーバ73及び第2サーバ74で暗号化されている。

次に、別のサーバで復号できるように再暗号化するための暗号化鍵取得方法について説明する：

図2に示す暗号化鍵取得方法の実施例では、送信元メタデータMD0を受信した第1サーバ72は、E1(DATA2)を復号化してDATA2を得る。つづいてDATA2を再度利用する別のサーバ用に暗号化するための鍵を得るために、別のサーバ情報を示すE3(DATA1)(図2では暗号化された事業者情報)を検索キーとし、第1サーバ72に接続された暗号化鍵データベース25aを検索し「Key2」という暗号化鍵を取得する。そしてこの「Key2」によってDATA2を暗号化しER(DATA2)を生成し、第1送信メタデータMD1とする。第1サーバ72は、E3(DATA1)をその情報のままで検索キーとして利用するだけで復号化することはできないため、DATA1の内容は第1サーバ72には秘匿される。

又、図 3 に示す暗号化鍵取得方法の別の実施例では、送信元メタデータ MD 0 を受信した第 1 サーバ 7 2 は、E 1 (DATA 2) を復号化して DATA 2 を得る。つづいて DATA 2 を再度利用する別のサーバ用に暗号化するための鍵を得るために、別のサーバ情報を示す E 3 (DATA 1) のみを暗号化サーバ 7 7 に送信する。暗号化サーバ 7 7 では、E 3 (DATA 1) を復号して DATA 1 を得る。次に DATA 1 を検索キーとして暗号化鍵データベース 2 5 a を検索し「Key 2」という暗号化鍵を取得する。そしてこの「Key 2」によって DATA 1 を暗号化し ER (DATA 1) を生成し第 1 サーバ 7 2 に返信する。

第 1 サーバ 7 2 は E 3 (DATA 1) を ER (DATA 1) に置換する。もう 1 つの処理として、第 1 サーバ 7 2 は暗号化サーバ 7 7 から「Key 2」を受信して DATA 2 を暗号化して ER (DATA 2) を生成する。

図 3 に示した実施例でも、E 3 (DATA 1) の内容である DATA 1 は第 1 サーバ 7 2 に秘匿になっている。又、暗号化サーバ 7 7 には E 3 (DATA 1) しか送信されない所以、他の情報は暗号化サーバ 7 7 に対して秘匿されている。

本発明の第1の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ76内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。

#### (第2の実施例)

本発明の第2の実施例に係る個人情報保護方式の具体例について、図4は、モバイル環境下でのウェアラブルコンピュータ（携帯情報端末）を用いたユビキタスコンピューティングにおける電子商取引の流れについて示している。図4に示す電子商取引システムは、第1のウェアラブルコンピュータ（携帯情報端末）10aと、個人認証サーバ26、端末認証サーバ27、事業者認証サーバ28からなるメタサーバ76と、個人認証サーバ26と端末認証サーバ27を接続する第1の匿名通信路71a、端末認証サーバ27と事業者認証サーバ28を接続する第2の匿名通信路71b、商品提供事業者50、そして商品提供事業者50が保有する事業者サーバ51からなる。

例示的な処理の流れは以下のようになる：

(a) まず第1のウェアラブルコンピュータ（携帯情報端末）10aより、個人情報、端末情報、事業者情報、商品情報等がメタサーバ76に送信される。

(b) 個人認証サーバ26は、受信したメタデータの内個人情報のみを復号化して、個人の正当性を認証する。個人認証サーバ26はその他の情報については知ることができない。

(c) 次に端末認証サーバ27は、第1の匿名通信路71aを経由して受信したメタデータの内端末情報のみを復号化して、端末の正当性を認証する。端末認証サーバ27はその他の情報については知ることができない。

(d) 次に事業者認証サーバ28は、第2の匿名通信路71bを経由して受信したメタデータの内事業者情報のみを復号化して、事業者の正当性を認証する。事業者認証サーバ28はその他の情報については知ることができない。

(e) メタサーバ76で必要な認証が完了すると、メタデータは商品提供事業者50の保有する事業者サーバ51へ送信される。事業者サーバ51では、商取引に必要な、個人情報や商品情報を復号して読み取り確認すると、商品の送付を行い商取引が完了する。

本発明の第2の実施例によれば、図4に示した流れの中では、メタサーバ76の個人認証サーバ26、端末認証サーバ27、事業者認証サーバ28のいずれのサーバ

も、ユーザは何を購入したかを知ることはいないし、どの商品提供事業者 50 との間で商取引を行っているのかも知ることはいない。この様に必要な認証を行いながらも、個人的な情報を秘匿したままで電子商取引を行うことができる。

### (第 3 の実施例)

本発明の第 3 の実施例に係る個人情報保護方式の具体例について、図 5 は、モバイル環境下でのコミュニティにおける情報交換の流れについて示している。図 5 に示す情報交換システムは、第 1 のウェアラブルコンピュータ（携帯情報端末）10a と第 2 のウェアラブルコンピュータ（携帯情報端末）10b、個人認証サーバ 26、送付先認証サーバ 29 からなるメタサーバ 76 と、個人認証サーバ 26 と送付先認証サーバ 29 の間に設けられた第 1 の匿名通信路 71a からなる。

例示的な処理の流れは以下のようなになる：

(a) 第 1 のウェアラブルコンピュータ（携帯情報端末）10a（会員 A）から、以下の情報を含む送信元メタデータ MD0 を送信する。

(i) 個人認証サーバ 26 で復号できる形に暗号化した会員 A 情報

(ii) 送付先認証サーバ 29 で復号できる形に暗号化



した会員 B のアドレス

(iii) 第 2 のウェアラブルコンピュータ (携帯情報端末) 10b (会員 B) で復号できる形に暗号化した秘密のメッセージ

(b) メタサーバ 76 の個人認証サーバ 26 が、受信した送信元メタデータ MD0 の中の会員 A 情報を復号化して個人認証を行う。その後、会員 A 情報を第 2 のウェアラブルコンピュータ 10b で復号できる形に再暗号化して置換する。そして生成されたメタデータを送付先認証サーバ 29 に送信する。

(c) 送付先認証サーバ 29 は、第 1 の匿名通信路 71a を経由してメタデータを受信する。そして送付先認証サーバ 29 で復号できる形に暗号化された会員 B のアドレスを復号し、会員 B がコミュニティの一員であるかどうかを認証する。正しく認証できた場合、送付先認証サーバ 29 は第 2 のウェアラブルコンピュータ 10b に向かってメタデータを送信する。

(d) 第 2 のウェアラブルコンピュータ 10b は受信したメタデータを復号して受信復号メタデータ MD4 を生成し、会員 A 情報と秘密のメッセージを表示又は音声等でユーザに通知する。

本発明の第 3 の実施例によれば、メタサーバ 76 の個人認証サーバ 26 で送信元を認証し、送付先認証サーバ 29 で送信先を認証するので、閉じられたコミュニティ

の会員同士の間に情報交換を限定することができる。この様に外部の人からの発言を阻止できる上に、誤って外部の人に情報が送信され読まれてしまうことも防止できる。又、個人認証サーバ26は、送信相手が誰なのかを知ることはないし、送付先認証サーバ29は送信元が誰なのかを知ることはない。よって、閉じられたメタサーバ76のサーバ同士でも個人間の情報を互いに秘匿状態にしたままやり取りができるので、個人情報の保護に優れている。

#### (第4の実施例)

本発明の第4の実施例に係る暗号化鍵取得システムは、図6に示すように、ユーザが利用する第1のウェアラブルコンピュータ(携帯情報端末)10aと、第1のウェアラブルコンピュータ10aから送信される送信元メタデータM.D0を処理する第1サーバ72と、第1サーバ72に接続された暗号化鍵データベース25aから構成される。但し、第1サーバ72は、複数のサーバからなるメタサーバの内のサーバの任意の1つとして説明する。

次に、図7を参照しながら本発明の第4の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

(a) まず、ステップS101において、第1のウェ

アラブルコンピュータ 10a のメモリ内に格納された固定乱数 RN により生成される検索タグ情報 CODE を暗号化した暗号化検索タグ情報 E (CODE) を含む送信元メタデータ MD0 を第 1 サーバ 72 が受信する。

(b) 次に、ステップ S102 において、送信元メタデータ MD0 から暗号化検索タグ情報 E (CODE2) を検索する。

(c) ステップ S102 において、暗号化検索タグ情報 E (CODE2) が検出されない場合は、ステップ 105 において、第 1 送信メタデータを次段以降のサーバに送信する。

(d) 一方、ステップ S102 において、暗号化検索タグ情報 E (CODE2) が検出されると、ステップ 103 において、検索タグ情報 CODE2 にあらかじめ関連づけられる関連情報である暗号化鍵データ Key2 が暗号化鍵データベース 25a から第 1 サーバ 72 へ送信される。次に、第 1 サーバ 72 は、E1 (DATA2) を復号化して DATA2 を処理後、ステップ 104 において、DATA2 を「Key2」によってサーバ R で読み取りが可能な情報に暗号化し ER (DATA2) を生成し、第 1 送信メタデータ MD1 内に格納する。次に、ステップ 105 において、第 1 サーバ 72 は、第 1 送信メタデータ MD1 を次段以降のサーバに転送する。

図 6 で示す「CODE2」は検索タグ情報であり、第

1 のウェアラブルコンピュータ 10 a に搭載されるメモリ領域に記録された固定乱数 R N を用いて生成される。固定乱数 R N は、ウェアラブルコンピュータ毎毎に特徴のある固有のデータであり、例えば 8 ビット、16 ビット、32 ビット 64 ビット等の特定の大きさを有する。固定乱数 R N は、検索タグ情報 C O D E 2 としてそのまま用いることも可能であるが、第 1 のウェアラブルコンピュータ 10 a の内部に記録される住所、電話番号、日付、時刻、氏名等の第 1 のウェアラブルコンピュータ 10 a に内蔵される情報を用いて加工されたデータであっても良い。「E (C O D E 2)」は検索タグ情報を暗号化したデータである。検索タグ情報 C O D E 2 を暗号化する手段 (モジュール) としては、住所、電話番号、日付、時刻、氏名等の第 1 のウェアラブルコンピュータ 10 a に内蔵される情報を用いて乱数を発生させることも可能である。

本発明の第 4 の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ 76 内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。更に、固定乱数 R N は、受信サーバ側で初めて意味のあるデータに変換されるため、より秘匿性を高めることができる。又、必要な個人

情報がサーバ側で管理されることと、固定乱数 R N のデータサイズが小さくて済むため、第 1 のウェアラブルコンピュータ 1 0 a 内の使用メモリ領域を節約することが可能となる。

#### (第 5 の実施例)

本発明の第 5 の実施例に係る暗号化鍵取得システムは、図 8 に示すように、ユーザが利用する第 1 のウェアラブルコンピュータ (携帯情報端末) 1 0 a と、第 1 のウェアラブルコンピュータ 1 0 a から送信される送信元メタデータ M D 0 を処理する第 1 サーバ 7 2 と、第 1 サーバ 7 2 に接続された暗号化情報データベース 2 5 から構成される。但し、第 1 サーバ 7 2 は、複数のサーバからなるメタサーバの内のサーバの任意の 1 つとして説明する。

次に、図 9 を参照しながら本発明の第 5 の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

( a ) まず、ステップ S 1 1 1 において、第 1 のウェアラブルコンピュータ 1 0 a のメモリ内に格納された固定乱数 R N により生成される検索タグ情報 C O D E を暗号化した暗号化検索タグ情報 E ( C O D E ) を含む送信元メタデータ M D 0 を第 1 サーバ 7 2 が受信する。

( b ) 次に、ステップ S 1 1 2 において、送信元メタデ

ータMD0から暗号化検索タグ情報E(CODE2)を検索する。

(c) ステップS112において、暗号化検索タグ情報E(CODE2)が検出されない場合は、ステップ114において、第1送信メタデータMD1を次段以降のサーバに送信する。

(d) 一方、ステップS112において、暗号化検索タグ情報E(CODE2)が検出されると、ステップ113において、検索タグ情報CODE2にあらかじめ関連づけられた関連情報である暗号化情報E2(INFO2)が第1送信メタデータMD1に格納される。次に、ステップS114において、第1送信メタデータMD1は次段以降のサーバに転送される。但し、暗号化情報E2(INFO2)は2段目のサーバで読取りが可能な暗号化情報データであるが、他のサーバの処理に必要な情報であっても良い。

本発明の第5の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ76内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。更に、固定乱数RNは、受信サーバ側で初めて意味のあるデータに変換されるた

め、より秘匿性を高めることができる。又、必要な個人情報サーバ側で管理されることと、固定乱数RNのデータサイズが小さくて済むため、第1のウェアラブルコンピュータ10a内の使用メモリ領域を節約することが可能となる。

#### (第6の実施例)

本発明の第6の実施例に係る暗号化鍵取得システムは、図10に示すように、ユーザが利用する第1のウェアラブルコンピュータ（携帯情報端末）10aと、第1のウェアラブルコンピュータ10aから送信される送信元メタデータMD0を処理する第1サーバ72と、第1サーバ72に接続された暗号化情報データベース25から構成される。但し、第1サーバ72は、複数のサーバからなるメタサーバの内のサーバの任意の1つとして説明する。ここでは、図8に示す「E1(DATA2)」をサービス情報として説明する。サービス情報は、商品やサービスの取引において必要な情報が含まれ、例えばサイズ、色等の商品情報、事業者情報、配送情報などが考えられる。

次に、図11を参照しながら本発明の第6の実施例に係る暗号化鍵取得方法について例示的な処理の流れを説明する：

(a) まず、ステップ S 1 2 1 において、サービス情報を暗号化した暗号化情報 E 1 (DATA 2)、及び第 1 のウェアラブルコンピュータ 1 0 a のメモリ内に格納された固定乱数 RN により生成される検索タグ情報 CODE 2 を暗号化した暗号化検索タグ情報 E (CODE 2) を含む送信元メタデータ MD 0 を第 1 サーバ 7 2 が受信する。但し、サービス情報としては、2 次元にコード化された情報等を第 1 のウェアラブルコンピュータ 1 0 a が光学的に読み込むことで取得したデータ等が考えられる。

(b) 次に、ステップ S 1 2 2 において、送信元メタデータ MD 0 から暗号化情報及び暗号化検索タグ情報を検索する。

(c) 次に、ステップ S 1 2 2 において、暗号化情報 E 1 (DATA 2) が検出された場合は、暗号化情報 E 1 (DATA 2) にあらかじめ関連づけられる第 2 データ変換テーブル 4 2 が選択される。次に、ステップ S 1 2 4 において、第 1 サーバ 7 2 は、ステップ S 1 2 4 において、送信元メタデータ MD 0 から暗号化検索タグ情報を検索する。一方、暗号化情報 E 1 (DATA 2) が検出されない場合は、そのまま第 1 サーバ 7 2 は、ステップ S 1 2 4 において送信元メタデータ MD 0 から暗号化検索タグ情報を検索する。

(d) ステップ S 1 2 4 において、暗号化検索タグ情報 E (CODE 2) が検出されない場合は、ステップ 1 2 6 において、第 1 送信メタデータ MD 1 を次段以降の



サーバに送信する。

(e) 一方、ステップ S 1 2 4 において、暗号化検索タグ情報 E (CODE 2) が検出されると、ステップ 1 2 5 において、検索タグ情報 CODE 2 にあらかじめ関連づけられた関連情報である暗号化情報 E 2 (INFO 2) が第 1 送信メタデータ MD 1 に格納される。次に、ステップ S 1 2 6 において、第 1 送信メタデータ MD 1 は次段以降のサーバに転送される。

本発明の第 6 の実施例によれば、各サーバは、サーバの処理に必要な情報のみを復号化して知ることができる。他の情報については受信しても内容は秘匿されたままにできるため、メタサーバ 7 6 内のサーバであっても不必要にのぞき見することはできない。したがって、個人情報等のセキュリティが確保され、安全にユビキタスコンピューティングを実現できる。

又、図 1 に示すユビキタスコンピューティングにおける個人情報保護方法が、個人情報、端末情報、事業者情報、商品情報等からなる送信元メタデータ MD 0 をメタサーバ 7 6 に転送していたのに対し、ウェアラブルコンピュータ 1 0 a 側で生成された検索タグ情報 CODE 2 を扱うため、個人情報、端末情報、事業者情報、商品情報等からなる送信元メタデータ MD 0 をウェアラブルコンピュータ 1 0 a 内に保存する必要がなくなり、ウェアラブルコンピュータ 1 0 a の内部で利用されるメモリ領

域を節約することができる。

(第7の実施例)

図12を参照して、本発明の第7の実施例に係る情報処理サーバ30と、情報処理サーバ30を利用した情報処理システムについて説明する。情報処理サーバ30は、中央処理制御装置、メモリなどを備える一般的なコンピュータに所定の処理を実行するソフトウェアプログラムをインストールすることによって実現される。

本発明の情報処理サーバ30は、第2通信端末(認証端末)20bが備える認証情報を利用して、認証情報を備えない第1通信端末20aを認証する。ここで、第1通信端末20aは、一般的なコンピュータで、第2通信端末(認証端末)20bは、認証情報を備えた携帯電話機などの通信端末である。認証情報は、指紋認証情報なのでも良いが、第7の実施例においては、情報処理サーバ30が発行した暗号化され改竄不可能な認証識別子であるとする。

第7の実施例に係る情報処理システムにおいて、情報処理サーバ30は、第1通信ネットワーク70aを介して第1通信端末20aと互いに接続可能で、更に、第2通信ネットワーク70bを介して第2通信端末(認証端末)20bと互いに接続可能である。第1通信ネットワーク70aと第2通信ネットワーク70bは、少なくとも

も一部が互いに交差しない通信ネットワークである。

第7の実施例に係る情報処理サーバ30は、認証パラメータ記憶装置101、認証情報記憶装置102、認証識別子記憶装置302b、画像生成手段(モジュール)32、認証情報取得手段(モジュール)112、認証情報照合手段(モジュール)113、入出力制御手段(モジュール)31を備えている。

認証識別子記憶装置302bは、情報処理サーバ30が発行した第2通信端末(認証端末)20bを認証するための認証識別子(認証情報)を記憶した記憶装置である。

画像生成手段(モジュール)32は、第1通信端末20aの認証依頼を受信すると、認証パラメータを生成し、認証パラメータを含む認証画像を生成して第1通信端末20aに送信し、認証パラメータを認証パラメータ記憶装置101に記憶させる手段である。

ここで、画像生成手段(モジュール)32で生成し、認証パラメータ記憶装置101に記憶される認証パラメータは、一意に特定できるワンタイムパスワードの様な乱数及び日時のいずれか1つ以上を含む情報である。この認証パラメータの「日時」は、認証パラメータ生成時の日時でも良いし、第1通信端末20aの認証依頼を受信した日時でも良い。又、認証パラメータ記憶装置101には、認証パラメータを有効にする期限である有効日時も記憶していても良い。画像生成手段(モジュール)

32は、第1通信ネットワーク70aを介して第1通信端末20aに認証画像を送信する。ここでは認証画像を送信すると記載したが、第2通信端末（認証端末）20bにおいて情報を解読できれば、テキストでも構わない。テキストの場合、簡単に盗聴できないような桁数の多いものが好ましい。

認証情報取得手段（モジュール）112は、第1通信端末20aから取得した認証画像の情報と、第2通信端末（認証端末）20bが備える認証情報を、第2通信端末（認証端末）20bから取得し、認証情報記憶装置102に記憶させる手段である。認証情報取得手段（モジュール）112は、第2通信ネットワーク70bを介して第2通信端末（認証端末）20bから認証情報を受信する。ここで、認証画像の情報は、第1通信端末20aから取得した認証画像を、第2通信端末（認証端末）20bにおいてデコードした情報であっても良いし、第1通信端末20aから取得し、第2通信端末（認証端末）20bから受信した認証画像を、情報処理サーバ30においてデコードした情報であっても良い。更に、第1通信端末20aから認証画像の情報を取得する場合、第2通信端末（認証端末）20bによって、第1通信端末20aに提示された認証画像を撮影しデコードしても良い。又、第1通信端末20aと第2通信端末（認証端末）20bの間で赤外線通信などの近距離無線通信を利用したり、リムーバブルディスクを利用して、第2通信端末（認

証端末) 20bは認証画像を取得しても良い。

認証情報照合手段(モジュール)113は、認証パラメータ記憶装置101と認証情報記憶装置102と認証識別子記憶装置302bを参照して、認証情報取得手段(モジュール)112で取得した認証画像の情報が、画像生成手段(モジュール)32で生成された画像の情報であり、更に、第2通信端末(認証端末)20bが備える認証情報が、認証識別子記憶装置302bに記憶した認証情報と一致するか否かを判定し、その結果を第1通信端末20aに送信する手段である。更に、認証パラメータ記憶装置101において、認証パラメータの有効日時が記憶されている場合、認証情報取得手段(モジュール)112で取得した日時が、認証パラメータ記憶装置101に記憶された認証パラメータの有効日時以前の場合に認証を許可し、認証パラメータの有効日時以降の場合に認証を不可にしても良い。

入出力制御手段(モジュール)31は、情報処理サーバ30の入力や出力を制御し、それぞれのネットワークや手段(モジュール)にその情報を伝達する手段である。

第7の実施例に係る第1通信端末20aは、画像データ記憶装置12a、画像取込手段(モジュール)11a、認証画像提示手段(モジュール)212、認証結果取得手段(モジュール)213を備えている。

画像取込手段(モジュール)11aは、情報処理サーバ30の画像生成手段(モジュール)32によって生成

された認証画像を取得し、画像データ記憶装置 12 a に記憶させる手段である。認証画像提示手段（モジュール）212 は、画像データ記憶装置 12 a に記憶された認証画像データを第 2 通信端末（認証端末）20 b に提示する手段である。

更に、認証結果取得手段（モジュール）213 は、情報処理サーバ 30 の認証情報照合手段（モジュール）113 によって送信された認証の結果を取得する手段である。

第 7 の実施例に係る第 2 通信端末（認証端末）20 b は、画像データ記憶装置 12 b、認証識別子記憶装置 302 a、画像取込手段（モジュール）311、認証情報送信手段（モジュール）312 を備えている。

画像取込手段（モジュール）311 は、第 1 通信端末 20 a の認証画像提示手段（モジュール）212 によって提示された画像を撮影し、画像データ記憶装置 12 b に記憶させる手段である。画像を撮影する必要はなく、第 1 通信端末 20 a に送信された認証画像を第 2 通信端末（認証端末）20 b に取得できればどのような手段（モジュール）を用いても構わない。

認証情報送信手段（モジュール）312 は、認証識別子記憶装置 302 a に記憶された、情報処理サーバ 30 から取得した認証識別子と、画像データ記憶装置 12 b に記憶された画像の情報を第 2 通信ネットワーク 70 b を介して情報処理サーバ 30 に送信する手段である。

次に、図 13 を参照して本発明の第 7 の実施例に係る情報処理方法を説明する：

(a) まず、ステップ S 201 において情報処理サーバ 30 は、画像生成手段 (モジュール) 32 によって、第 1 通信端末 20a から認証依頼を受信すると、ステップ S 202 において、ワンタイムパスワードや日時などの情報を含む認証画像を生成し、認証パラメータ記憶装置 101 に記憶する。更にステップ S 203 において、情報処理サーバ 30 は、生成した認証画像を第 1 通信端末 20a に送信する。

(b) 第 1 通信端末 20a は、ステップ S 203 において認証画像を受信すると、受信した画像をステップ S 204 において提示する。

(c) ステップ S 204 において第 1 通信端末 20a で認証画像が提示されると、ステップ S 205 において第 2 通信端末 (認証端末) 20b は提示された認証画像を撮影し、画像データ記憶装置 12b に記憶する。更にステップ S 206 において第 2 通信端末 (認証端末) 20b は、画像データ記憶装置 12b に記憶された認証画像の情報と、認証識別子記憶装置 302a に記憶された第 2 通信端末 (認証端末) 20b の認証識別子を併せて認証情報を作成し、ステップ S 207 において、認証情報を情報処理サーバ 3007 に送信する。

(d) ステップ S 207 において、情報処理サーバ 3

0 は第 2 通信端末（認証端末）20b から認証情報を受信すると、認証情報取得手段（モジュール）112 によって、受信した認証情報を認証情報記憶装置 102 に記憶し、ステップ S208 において認証情報照合手段（モジュール）113 によって認証パラメータ記憶装置 101、認証情報記憶装置 102、認証識別子記憶装置 302b を参照して認証情報の照合を行う。

（e）認証情報の認証結果が出ると、情報処理サーバ 30 は、第 1 通信端末 20a に認証結果を送信し、第 1 通信端末 20a は認証結果取得手段（モジュール）213 によって認証結果を受信する。

本発明の第 7 の実施例に係る情報処理サーバ 30 によると、第 2 通信端末（認証端末）20b の認証情報を利用することにより、認証情報を備えていない第 1 通信端末 20a を認証することができる。したがって、ユーザは 1 つの第 2 通信端末（認証端末）20b を備えていれば、複数の端末について同様に認証を受けることができる。

更に、本発明の第 7 の実施例によれば、本来は携帯電話機で入力しなければならない情報を、ユーザインターフェースの充実しているコンピュータで入力し、更に、セキュリティレベルの高い状態で、その入力した情報をサーバに送信することができる。



### (第 8 の実施例)

図 1 4 に示した本発明の第 8 の実施例に係る情報処理システムは、図 1 2 に示した本発明の第 7 の実施例に係る情報処理システムに比べて、コンテンツ提供サーバ 5 を備えている点が異なる。更に、第 1 通信端末 2 0 a において、認証結果取得手段（モジュール）2 1 3 を備えておらず、コンテンツ取得手段（モジュール）2 1 4 を備えている点が異なる。

本発明の第 8 の実施例に係る情報処理サーバ 3 0 は、画像生成手段（モジュール）3 2 において、コンテンツ提供サーバ 5 から、第 1 通信端末 2 0 a の認証依頼を受信し、認証情報照合手段（モジュール）1 1 3 において、結果をコンテンツ提供サーバ 5 に送信する。

本発明の第 8 の実施例に係るコンテンツ提供サーバ 5 は、情報処理サーバ 3 0 及び第 2 通信端末（認証端末）2 0 b の情報を利用して第 1 通信端末 2 0 a を認証し、認証された第 1 通信端末 2 0 a にコンテンツを配信するものであって、コンテンツ記憶装置 5 0 1、認証依頼手段（モジュール）5 1 1、認証結果取得手段（モジュール）5 1 2、コンテンツ配信手段（モジュール）5 1 3 を備えている。

コンテンツ記憶装置 5 0 1 は、コンテンツ提供サーバ 5 が提供するコンテンツが記憶された記憶装置である。

認証依頼手段（モジュール）5 1 1 は、例えば第 1 通

信端末 20 a からコンテンツの取得依頼があると、情報処理サーバ 30 に対して、第 1 通信端末 20 a の認証を依頼する手段である。

認証結果取得手段（モジュール）512 は、認証依頼手段（モジュール）511 で依頼した第 1 通信端末 20 a の認証結果を、情報処理サーバ 30 から取得する手段である。

コンテンツ配信手段（モジュール）513 は、第 1 通信端末 20 a が認証されると、コンテンツ記憶装置 501 に記憶されたコンテンツを第 1 通信端末 20 a に送信する手段である。

図 14 においては、本発明の第 8 の実施例に係るコンテンツ提供サーバ 5 は、第 1 通信ネットワーク 70 a に接続されているが、情報処理サーバ 30 と相互に通信可能ならば、どの通信ネットワークに接続されても良い。

図 15 を参照して、本発明の第 8 の実施例に係る情報処理方法を説明する：

（a）まず、ステップ S302 において、第 1 通信端末 20 a からコンテンツ提供サーバ 5 にコンテンツの要求がされると、コンテンツ提供サーバ 5 は、ステップ S302 において認証依頼手段（モジュール）511 によって、情報処理サーバ 30 に第 1 通信端末 20 a の認証を依頼する。

（b）その後、ステップ S303 乃至ステップ 209

の処理は、図 13 のステップ S 202 乃至ステップ S 208 の処理と同様なので説明を割愛する。

(c) ステップ S 309 において、情報処理サーバ 30 において認証結果が出ると、情報処理サーバ 30 はステップ S 310 において、第 1 通信端末 20a の認証結果をコンテンツ提供サーバ 5 に送信する。

(d) コンテンツ提供サーバ 5 は、認証が許可されると、ステップ S 311 においてコンテンツ記憶装置 501 から第 1 通信端末 20a にコンテンツを提供する。

この方法は、第 1 通信端末 20a において一般的なブラウザを利用してコンテンツ提供サーバ 5 からコンテンツを取得する場合に有効である。

次に、図 16 を参照して、本発明の第 8 の実施例の変形例に係る情報処理方法について説明する。

(a) まず、ステップ S 351 において、第 1 通信端末 20a がコンテンツ提供サーバ 5 にコンテンツを要求すると、ステップ S 352 において、コンテンツ提供サーバ 5 は、第 1 通信端末 20a に認証情報を要求する。

(b) これを受けて第 1 通信端末 20a は、ステップ S 353 において情報処理サーバ 30 に認証依頼を行う。

(c) その後、ステップ S 354 乃至ステップ S 260 の処理は、図 13 のステップ S 202 乃至ステップ S 208 の処理と同様なので説明を割愛する。

(d) ステップ S 360 において、情報処理サーバ 3

0 において認証結果が出ると、情報処理サーバ 30 はステップ S 3 6 1 において、第 1 通信端末 20 a の認証結果を第 1 通信端末 20 a に送信し、これを受けて第 1 通信端末 20 a は、ステップ S 3 6 2 において認証結果をコンテンツ提供サーバ 5 に送信する。

(e) コンテンツ提供サーバ 5 は、認証結果を受信すると、認証が許可されている場合、ステップ S 3 6 3 においてコンテンツ記憶装置 501 から第 1 通信端末 20 a にコンテンツを提供する。

この方法は、第 1 通信端末 20 a において、コンテンツ提供サーバ 5 や情報処理サーバ 30 が提供する認証依頼プログラムを含むアプリケーションによって、コンテンツ提供サーバ 5 にコンテンツを提供する場合に有効である。

本発明の第 8 の実施例によれば、情報処理サーバ 30 は、複数のサーバの認証機能を受け付けることができ、様々なサーバに高いセキュリティレベルの認証を行わせることができる。

#### (第 9 の実施例)

本発明の第 1 及び第 8 の実施例においては、第 1 通信端末 20 a の認証について主に説明したが、本発明の第 9 の実施例においては、第 1 通信端末 20 a 及び第 2 通信端末 (認証端末) 20 b を操作するユーザの認証につ

いて説明する。

図 1 7 に示す本発明の第 9 の実施例に係る情報処理サーバ 3 0 は、図 1 2 に示す本発明の第 7 の実施例に係る情報処理サーバ 3 0 と比べて、リマインダー質疑応答記憶装置 1 0 4、リマインダー質疑応答登録手段（モジュール） 1 1 4、パスワード再発行手段（モジュール） 1 1 5 を備えている点が異なる。更に、第 9 の実施例に係る第 2 通信端末（認証端末） 2 0 b は、第 7 の実施例に係る第 2 通信端末（認証端末） 2 0 b に比べて、リマインダー質疑応答登録手段（モジュール） 3 1 3、再発行パスワード取得手段（モジュール） 3 1 4 を備えている点が異なる。

リマインダー質疑応答登録手段（モジュール） 1 1 4 は、第 2 通信端末（認証端末） 2 0 b のリマインダー質疑応答登録手段（モジュール） 3 1 3 によって複数ある質疑応答の内、ユーザにユーザが答えられる複数の質疑応答を選択させ、ユーザの認証識別子に関連づけて、そのユーザが選択した質疑応答とその答えをリマインダー質疑応答記憶装置 1 0 4 に記憶させる手段である。

パスワード再発行手段（モジュール） 1 1 5 は、ユーザがパスワードを忘れてしまった場合、第 2 通信端末（認証端末） 2 0 b の再発行パスワード取得手段（モジュール） 3 1 4 によってパスワードの再発行が要求されると、リマインダー質疑応答記憶装置 1 0 4 を参照してユーザが選択した質問をユーザに答えさせ、リマインダー質疑

応答記憶装置 104 に記憶された応答と一致するかを判定し、全ての質疑に答えられた場合、ユーザにパスワードを発行する手段である。

図 18 に示すように、本発明の第 9 の実施例の情報処理サーバ 30 が提示する複数の質疑応答は、質疑の候補、応答のセレクトリストの項目を備えている。更に、質疑のジャンルとセレクトリストのセレクト数の項目を備えていても良い。ユーザはこれらの質疑の候補の中から、ユーザ自身が確実に答えられる質問を所定の数（例えば 4 つなど）以上を、ユーザに選択させる。この様にユーザが登録時に 4 問以上選択することになる場合、11 問から 4 問以上を選択する組合せの数は、1817 通りとなる。

例えば、「お母さんは何日生まれ？」という質問がユーザに選択されたとすると、セレクトリストとしては 1 ～ 31 日が挙げられ、ユーザはその中から正解を選択する。これらを所定の数だけ繰り返し、第 2 通信端末（認証端末）20b は、情報処理サーバ 30 に送信する。例えば、選択数 15 の質疑をユーザが 4 つ選択したとすると、その回答の組合せは、15 の 4 乗となり、50625 通りにも及ぶ。このような方法を取ることで、ユーザの選択した質疑とその応答を解読するのは不可能になり、より高いセキュリティレベルを保つことができる。

例えば、図 19 に示すように、英数字だけのパスワードによると、英数字（A ～ Z までの英字 26 文字と 0 か

ら 9 までの数字 10 個) を組合せると、36 文字の 4 乗で 1, 679, 616 通りあることを示す。

一方、本発明の第 9 の実施例で説明した方法によると、図 18 に示す様に 11 の質問から 4 つを選択し、その 4 つについて 50, 625 通りのセレクトリストの組合せがあるとする、ユーザが取り得る組合せは、少なく見積もっても 91, 985, 625 通り以上となる。これは、図 19 を参照すると分かるように、英数字のみをパスワードにした場合、5～6 桁の、数字のみをパスワードにした場合、7～8 桁の強度があることが分かる。

図 20 を参照して、本発明の第 9 の実施例に係る情報処理方法について説明する：

(a) まず、リマインダー質疑応答を登録する場合、ステップ S401 において情報処理サーバ 30 は第 2 通信端末 (認証端末) 20b に質問と、回答の選択肢の組合せを送信し、ユーザに確実に回答できる質問とその答えを決定させる。次に、ステップ S402 において、情報処理サーバ 30 は第 2 通信端末 (認証端末) 20b から、所定の数以上の質問と回答の組合せを受信し、リマインダー質疑応答記憶装置 104 に記憶する。

(b) 更にパスワードを再発行する場合、ステップ S451 において、情報処理サーバ 30 は第 2 通信端末 (認証端末) 20b からパスワードの再発行依頼を受信すると、ステップ S452 において、情報処理サーバ 30 は

第 2 通信端末（認証端末）20b に、ステップ S 401 で送信した質問と回答の選択肢の組合せと同じものを送信し、ユーザにステップ S 402 で回答した質問に回答させる。

（c）更に、ステップ S 453 において、第 2 通信端末（認証端末）20b から登録時に回答した質問と回答の組合せを受信すると、ステップ S 454 においてリマインダー質疑応答記憶装置 104 を参照して回答を照合し、照合の結果、選択した質問と、その質問の回答の全てが一致していた場合、ステップ S 453 においてパスワードを再発行する。

本発明の第 9 の実施例に係る情報処理システムによれば、非常に高いセキュリティレベルでユーザを認証することができる。

#### （第 10 の実施例）

本発明の第 10 の実施例に係る情報処理サーバ 30a は、図 21 に示すように、通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置 34 と、通信端末から入力される情報を、対応情報に従って変換する情報変換手段（モジュール）33 とを備える。更に、通信端末から入力される情報から画像を作成する画像生成手段（モジュール）32 と、通信端末との情報



のやり取りを制御する入出力制御手段（モジュール）31とを備える。

識別子対応情報記憶装置34には、通信端末の機種等を認識するための識別子をしたがって、情報を送信する際にどのように変換すれば良いかを規定した対応情報が格納されている。

情報変換手段（モジュール）33は、識別子対応情報記憶装置34から対応情報を読み出し、該当の通信端末に送る情報を実際に変換する。画像生成手段（モジュール）32は、通信端末内に画像作成機能がない場合に、情報を画像化して通信端末に送信する。

本発明の第10の実施例に係る情報処理システムでは、例えば図21に示すように、情報処理サーバ30aに、第1通信ネットワーク70aを介して第1通信端末20aが接続し、更に、第2通信ネットワーク70bを介して第2通信端末20bが接続している。更に複数の通信端末が複数の通信ネットワークを介して接続しても構わない。

第1通信端末20a及び第2通信端末20bは、情報を二次元コード化して紙面等に記載された画像を読み取るためのカメラやスキャナ等の画像取込手段（モジュール）11a、21を備える。更に読み取った画像情報を格納しておく画像データ記憶装置12a、22を備える。又、通信端末の機種等を認識させるための識別子情報を格納しておく識別子情報記憶装置を備える。そして、情

報処理サーバ30aと通信知るための情報送受信手段（モジュール）と、受信した画像等の情報を表示するための画像表示画面とを備える。

次に、図22を参照しながら、通信の手順を説明すると以下のようになる：

（a）ステップS500において、第1通信端末20aは、二次元コード化された画像を画像取込手段（モジュール）11aによって端末内に取り込み、第1通信端末20a自体の情報と共に情報処理サーバ30aに送信する。

（b）ステップS501において、情報処理サーバ30aは、第1通信端末20aから受信した情報を元に、二次元コード化した画像の情報を第1通信端末20aに返信する：

ステップS502において、第1通信端末20aは、情報処理サーバ30aから受信した画像を画像表示画面15aに表示する。

（c）ステップS503において、つづいて、第2通信端末20bは、第1通信端末20aの画像表示画面15aに表示された画像を、画像取込手段（モジュール）11bによって端末内に取り込み、識別子情報記憶装置13bに格納された識別子情報と共に情報処理サーバ30aに送信する。

（d）ステップS504において、情報処理サーバ3

0 a は、第 2 通信端末 2 0 b から受信した識別子を元に、識別子対応情報記憶装置 3 4 を検索し、情報を変換するための対応情報を読み出す。そして、その対応情報に従って情報を変換し、第 2 通信端末 2 0 b に返信する。

この手順のステップ S 5 0 4 の情報変換によって、異機種間の二次元コード化の記述方式の差分を吸収できるため、第 1 通信端末 2 0 a と第 2 通信端末 2 0 b が異機種でも、二次元コード化した画像を介して、必要な情報を正常に伝達することができる。

#### < 第 1 0 の実施例の具体例 1 : 電話番号交換 >

( a ) ステップ S 5 0 0 で、電話帳登録処理命令情報を二次元コード化した画像を読み取り、第 1 通信端末 2 0 a 自体の情報として、電話番号やメールアドレスを情報処理サーバ 3 0 a に送信する。

( b ) ステップ S 5 0 1 では、電話帳登録処理命令情報と第 1 通信端末 2 0 a の電話番号やメールアドレスを一体にして二次元コード化した画像が第 1 通信端末 2 0 a に返信される。

( c ) ステップ S 5 0 2 、ステップ S 5 0 3 では、第 1 通信端末 2 0 a の画像表示画面 1 5 a に表示された画像を第 2 通信端末 2 0 b で取り込み、第 2 通信端末 2 0 b の識別子と共に情報処理サーバ 3 0 a に送信する。

( d ) ステップ S 5 0 4 で、情報処理サーバ 3 0 a で

受信した画像は、第2通信端末20bが解釈できる情報に変換される。そしてその情報を受信した第2通信端末20bでは、電話帳に第1通信端末20aの電話番号やメールアドレスが登録させる。

同じ手順で、第2通信端末20bの電話番号やメールアドレスを、第1通信端末20aの電話帳に登録することで名刺交換と同様のことが二次元コード化画像を夜に込むことで可能になる。又、第2通信端末20bが画像生成機能を備えている場合は、第1通信端末20aの機種情報を得ておけば、第2通信端末20b内で画像を生成して、第1通信端末20aに直接読込ませることで、情報を伝達することができる。

#### < 第10の実施例の具体例2：複数端末情報 >

(a) ステップS500で、相性占い処理命令情報を二次元コード化した画像を読み取り、第1通信端末20a自体の情報として、生年月日や名前を情報処理サーバ30aに送信する。

(b) ステップS501では、相性占い処理命令情報と第1通信端末20aの生年月日や名前を一体にした情報か途中の占い結果を二次元コード化した画像が、第1通信端末20aに返信される。

(c) ステップS502、ステップS503では、第1通信端末20aの画像表示画面15aに表示された画

像を第2通信端末20bで取り込み、第2通信端末20bの情報として、識別子と生年月日や名前を共に情報処理サーバ30aに送信する。

(d) ステップS504での情報変換では、第2通信端末20bからの情報を元に相性占いプログラムを実行した結果を第2通信端末20bに返信する。更に第1通信端末20aにも結果を返信しても良い。

#### (第11の実施例)

本発明の第11の実施例に係る情報処理サーバ30bは、図23に示すように、第10の実施例に係る情報処理サーバ30aに、通信端末が情報交換を許可されているか示す許可情報を格納する許可情報記憶装置36と、許可情報を判定する許可判定手段(モジュール)35とを更に備えたものである。

許可情報記憶装置36は、各端末の電話番号や端末番号等の識別情報で検索することで読み出すことができる、通信許可/不許可を規定している情報を格納している。そして許可判定手段(モジュール)35は、その許可情報を読み出し、通信をしてよいかを判定し、許可なら処理を続行させ、不許可ならエラー処理を行う。

本発明の第11の実施例に係る情報処理システムは、図23に示すように、第10の実施例に係る情報処理システムと同様である。

次に、図 2 4 及び図 2 5 を参照しながら、通信の手順を説明すると以下のようなになる：

( a ) ステップ S 6 0 0 からステップ S 6 0 3 までは、図 2 2 のステップ S 5 0 0 からステップ S 5 0 3 までと同様である。

( b ) ステップ S 6 0 4 において、情報処理サーバ 3 0 b は、第 2 通信端末 2 0 b の識別情報を元に許可情報記憶装置 3 6 から許可情報を読み出す。その許可情報を許可判定手段（モジュール） 3 5 によって判定する。

( c ) ステップ S 6 0 5 において、もし情報の交換が許可されている場合、図 2 2 のステップ S 5 0 4 と同様に、情報処理サーバ 3 0 b は、識別子対応情報記憶装置 3 4 を検索し、情報を変換するための対応情報を読み出す。そして、その対応情報に従って情報を変換し、第 2 通信端末 2 0 b に返信する。

( d ) ステップ S 6 0 6 において、もし情報の交換が不許可の場合、エラー情報を第 2 通信端末 2 0 b に返信する。

この手順により、情報を共有できる端末、できない端末とグループ化することができ、情報のセキュリティを高めることができる。又、アクセス時刻等の情報をキーとして許可情報を許可情報記憶装置 3 6 に格納しておくことも可能である。これによって時間帯による規制等かけることができる。

(第12の実施例)

図26は、インターネット（通信ネットワーク）70に接続される携帯情報端末（第1端末）20と、事業者サーバ（第2端末）51と、情報処理サーバ30とに着目した本発明の第12の実施例に係る情報処理システムの構成図である。ここで、「携帯情報端末（第1端末）20」とは、第1～第11の実施例で説明したと同様な、カメラ、赤外線スキャナなど各種スキャナを含む種々の画像コード読取装置19を備える携帯情報端末である。

「画像コード」も、第1～第11の実施例でと同様な、一次元コード、二次元コード、ホログラムコード、ウォーターマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等を含むものである。具体的には、「画像コード」の一例として、QRコードと呼ばれるマトリクス型の二次元コードである情報コードと、情報コードの周囲を取り囲むように配置された識別力を有する情報コードとで構成しても良い。情報コードの一辺の長さは、例えば、8～15mm（外側のマージン込みで10～18mm）程度にすることが可能である。QRコードの他、情報コードとしては、国際標準規格になっているCode 16、Code 49、MaxiCode、Data Matrix、Code One等の二次元コード、或いはスキントークコードを用いても良い。識別コードは、

例えば、情報コードの周囲の空白部分の長さを、セルの一辺の４倍の長さとすることができる。ここで、「セル」とは、情報コードの最小描画単位を指す。

現実には、インターネット（通信ネットワーク）７０には、複数の事業者サーバ（第２端末）５１と、複数の携帯情報端末（第１端末）２０が接続されうるが、説明を簡単にするために、単一の事業者サーバ（第２端末）５１と、単一の携帯情報端末（第１端末）２０を図示している。本発明の第１２の実施例に係る情報処理システムは、やり取りをしたい携帯情報端末（第１端末）２０と事業者サーバ（第２端末）５１が認証する際に、携帯情報端末（第１端末）２０と事業者サーバ（第２端末）５１の間に別の認証のための情報処理サーバ３０が仲介して認証を行う方式である。実際には、携帯情報端末（第１端末）２０は、デジタル通信網（他の通信ネットワーク）に接続され、このデジタル通信網が中継処理装置を介して、インターネット（通信ネットワーク）７０に接続される構成で構わない。デジタル通信網には複数の移動通信加入者交換機が接続され、この移動通信加入者交換機には複数の無線中継機が接続されるようなシステム構成等でも良い。即ち、携帯情報端末（第１端末）２０から発信された情報は、無線中継機を介し、移動通信加入者交換機に送信され、この移動通信加入者交換機からデジタル通信網を介して中継処理装置に情報が送信され、この中継処理装置が、通信ネットワーク７０とデジタル



通信網のデータの仲介を行うようなシステムを図 2 6 は含み得ると理解すべきである。

図 2 6 に示した情報処理サーバ 3 0 は、アクション要求受信手段（モジュール）3 2 1 と、事業者サーバ認証手段（モジュール）3 2 2 と、個人・端末認証手段（モジュール）3 2 3 と、整理券情報発行手段（モジュール）3 2 4 と、整理券情報認証手段（モジュール）3 2 5 と、個人情報送信許可手段（モジュール）3 2 6 と、必要最小限情報送信手段（モジュール）3 2 7 とを有する CPU 3 2 0 を備える。更に、この CPU 3 2 0 には、事業者情報登録装置 3 7 と、個人情報登録装置 3 8 と整理券情報記憶装置 3 9 が接続されている。

ここで、アクション要求受信手段（モジュール）3 2 1 は、携帯情報端末（第 1 端末）2 0 からのアクション要求の受信をする手段である。又、事業者サーバ認証手段（モジュール）3 2 2 は、事業者サーバ（第 2 端末）5 1 の認証をする論理回路で、個人・端末認証手段（モジュール）3 2 3 は、携帯情報端末（第 1 端末）2 0 の認証をする論理回路で、整理券情報発行手段（モジュール）3 2 4 は、アクション要求を行った携帯情報端末（第 1 端末）2 0 に認証情報（整理券情報）を発行する論理回路で、整理券情報認証手段（モジュール）3 2 5 は、認証情報（整理券情報）が正しいか判定する論理回路である。更に、個人情報送信許可手段（モジュール）3 2

6 は、個人情報 の 送信 を 許可 する 論理 回路 で、 必要 最小 限 情報 送信 手段 (モジュール) 3 2 7 は、 認証 情報 (整理 券 情報) に 基づき、 要求 された アクション に 必要 最小 限 の 情報 のみ を 事業者 サーバ (第 2 端末) 5 1 に 送信 する 論理 回路 である。 一方、 事業者 情報 登録 装置 3 7 は 事業者 情報 を 記憶 する 記憶 装置 である。 又、 個人情報 登録 装置 3 8 は、 認証 対象 となる 個人情報 記憶 する 記憶 装置 である。 整理 券 情報 記憶 装置 3 9 は、 発行 する 認証 情報 (整理 券 情報) を 記憶 する 記憶 装置 である。

一方、 携帯 情報 端末 (第 1 端末) 2 0 は、 上記 の 画像 コード 読取 装置 1 9 に 加え、 処理 制御 装置 2 1、 画像 表示 装置 1 5、 画像 データ 記憶 装置 1 2 及び 個人情報 記憶 装置 1 8 等を 備える。 処理 制御 装置 2 1 は、 画像 取込 手段 (モジュール) 1 1 と、 画像 コード 解読 手段 (モジュール) 1 3 と、 画像 コード 変換 手段 (モジュール) 1 4 と、 統合 データ 編集 手段 (モジュール) 1 6 と、 電話 機能 制御 手段 (モジュール) 1 7 とを 有する。 この 処理 制御 装置 2 1 には、 画像 コード 読取 装置 1 9 と、 画像 表示 装置 1 5 と、 画像 データ 記憶 装置 1 2 と、 個人情報 記憶 装置 1 8 とが 接続 されている。

処理 制御 装置 2 1 の 画像 コード 解読 手段 (モジュール) 1 3 は、 画像 コード 読取 装置 1 9 で 読込まれた データ を 取得 し、 2 次元 コード 等の 画像 コード が 正当 である か どうか の チェック を 行う。 画像 コード 変換 手段 (モジュール) 1 4 は、 画像 コード 解読 手段 (モジュール) 1 3 で

読込まれた画像コードを文字データに変換する。画像コード解読手段（モジュール）13及び画像コード変換手段（モジュール）14を経ることによって、画像コードは、単なる画像データからコンピュータ読み取り可能なデータに変換することができる。統合データ編集手段（モジュール）16は、個人情報記憶装置18に記憶された個人情報と、画像コード変換手段（モジュール）14より得られた商品情報を編集統合し、外部に発信する手段（モジュール）である。画像コード読取装置19は、広告媒体に書かれた商品掲載ページ、商品情報などの商品に関する情報が埋め込まれた画像コードを読み取り、本発明の第12の実施例に係る携帯情報端末（第1端末）20に取り込むものである。

個人情報記憶装置18は、所有者（ユーザ）の個人情報を「第1レベルの個人情報」と「第2レベルの個人情報」とに分けて記憶する。「第1レベルの個人情報」とはユーザの氏名や登録番号等の携帯情報端末（第1端末）20の認証に必要な最低限の情報で、セキュリティレベルの低い個人情報である。「第2レベルの個人情報」とは第1レベルの個人情報よりもセキュリティレベルが高く、重要な個人情報で、例えば、住所、電子メールアドレス、クレジットカード番号、銀行口座名、給与、資産、家族構成の情報、身体的特徴等が含まれる。一時記憶装置は、画像コード読取装置19から読み取られたコードや、画像コード解読手段（モジュール）13及び画像

コード変換手段（モジュール）１４で得られるコードを一時保存するための記憶装置である。図２６には特に表示していないが、入力装置、無線装置、音声処理装置、CODEC（コーデック）、データ記憶装置、一時記憶装置、及びこれらの各装置が正常に機能するための電源回路や電池（バッテリー）等が備えられていることは勿論である。

図２７のフローチャートを用いて、本発明の第１２の実施例に係る情報処理方法を説明する：

（ａ）まず、ステップＳ７０１において、携帯情報端末（第１端末）２０は、紙媒体等に印刷された画像コードを読み取り、個人情報記憶装置１８に記憶された第１レベルの個人情報と、画像コードに含まれる商品情報を編集統合した統合情報を、アクション要求を仲介するサーバである情報処理サーバ３０に送信する。そして、ステップＳ７０２において、情報処理サーバ３０は携帯情報端末（第１端末）２０からのアクション要求の受信をする。

（ｂ）その後、ステップＳ７０３において、情報処理サーバ３０は、事業者情報登録装置３７及び個人情報登録装置３８に記録された内容を参照して、事業者サーバ（第２端末）５１の認証及び携帯情報端末（第１端末）２０の認証をする。

（ｃ）ステップＳ７０３において、事業者サーバ（第

2 端末) 5 1 の認証と携帯情報端末 (第 1 端末) 2 0 の認証ができれば、ステップ S 7 0 4 において、情報処理サーバ 3 0 はアクション要求を行った携帯情報端末 (第 1 端末) 2 0 に認証情報 (整理券情報) を発行する。更に、発行した認証情報 (整理券情報) を整理券情報記憶装置 3 9 に記憶する。

(d) 即ち、安全を確認できれば、携帯情報端末 (第 1 端末) 2 0 からの第 2 レベルの個人情報の送信が許可される。すると、ステップ S 7 0 5 において、携帯情報端末 (第 1 端末) 2 0 は、情報処理サーバ 3 0 に対し、この第 2 レベルの個人情報を認証情報 (整理券情報) と共に送信する。第 2 レベルの個人情報は、個人情報記憶装置 1 8 に記憶されているものの他、携帯情報端末 (第 1 端末) 2 0 の入力装置を用いて、新たに入力された必要最小限の情報でも良い。

(e) 次に、情報処理サーバ 3 0 は、第 2 レベルの個人情報と認証情報 (整理券情報) とを受信する。そして、ステップ S 7 0 6 において、受信した認証情報 (整理券情報) に基づき、要求されたアクションに必要な最小限の情報 (第 2 レベルの個人情報) のみを事業者サーバ (第 2 端末) 5 1 に送る。

図 2 7 に示す第 1 2 の実施例に係る情報処理方法によれば、不必要なデータを送信せず、かつお互いの不必要な情報を入手しなくても携帯情報端末 (第 1 端末) 2 0 と事業者サーバ (第 2 端末) 5 1 間の認証を可能とする。

図 28 は、第 12 の実施例に係る情報処理方法の実施に用いる情報処理サーバ 30 の動作を説明するフローチャートである。

(a) まず、ステップ S 711 において、情報処理サーバ 30 のアクション要求受信手段 (モジュール) 321 は、携帯情報端末 (第 1 端末) 20 からのアクション要求の受信を第 1 レベルの個人情報とともにする。そして、ステップ S 712 において、事業者サーバ認証手段 (モジュール) 322 は事業者サーバ (第 2 端末) 51 の認証をする。更に、ステップ S 713 において、個人・端末認証手段 (モジュール) 323 が携帯情報端末 (第 1 端末) 20 の認証をする。

(b) ステップ S 712 における事業者サーバ (第 2 端末) 51 の認証、及びステップ S 713 における携帯情報端末 (第 1 端末) 20 の認証が完了したら、ステップ S 714 において、情報処理サーバ 30 の整理券情報発行手段 (モジュール) 324 は、アクション要求を行った携帯情報端末 (第 1 端末) 20 に認証情報 (整理券情報) を発行する。

(c) ステップ S 715 において、情報処理サーバ 30 の整理券情報認証手段 (モジュール) 325 は、認証情報 (整理券情報) が正しいか判定し、正しいければ、ステップ S 716 において、個人情報送信許可手段 (モジュール) 326 は、第 2 レベルの個人情報の送信を携帯

情報端末（第１端末）２０に許可する。

（ｄ）情報処理サーバ３０は、この第２レベルの個人情報（整理券情報）と共に受信する。そして、ステップＳ７１７において、情報処理サーバ３０の必要最小限情報送信手段（モジュール）３２７は、認証情報（整理券情報）に基づき、携帯情報端末（第１端末）２０から要求されたアクションに必要な最小限の情報（第２レベルの個人情報）のみを事業者サーバ（第２端末）５１に送信する。

第１２の実施例に係る情報処理システムは、携帯情報端末２０に「エンクリプティッド・ランダムナンバー・メタデータベースシステム」を採用しても良い。「エンクリプティッド・ランダムナンバー・メタデータベースシステム」とは、携帯情報端末２０の個人情報記憶装置１８に「第１レベルの個人情報」の代わりに固有の無限に長い乱数の組を保持し、動的に発行するセッションＩＤと組み合わせ、情報処理サーバ３０でこの識別情報を個人情報に変換する方式である。

図２７のフローチャートにおけるステップＳ７０３又は図２８のフローチャートにおけるステップＳ７１２でアクションを要求する際、個人・端末認証のため、携帯情報端末２０から、携帯情報端末２０固有の情報や個人認証のための第１レベルの個人情報を受信する必要がある。エンクリプティッド・ランダムナンバー・メタデー

データベースシステムを用いることにより、携帯情報端末 20 から最初に発信される第 1 レベルの個人情報 は乱数であるため、安全に、より情報が第 3 者に不当に漏れないシステムとなる。

図 26 に示した第 12 の実施例に係る情報処理システムにおいて、情報処理サーバ 30 を、第 1 の実施例に係る個人情報保護方式のメタサーバ 76 と同様に、各処理毎に分割し、複数のサーバ 72, 73, 74 として実装し、通信ネットワーク 70 上に出回るデータはそのデータを処理するサーバのみで復号できる形で暗号化することによって、分割されたサーバでは処理に必要なデータ以外は復号化できないようにすることができる（図 1 参照。）。

即ち、図 26 に示す情報処理サーバ 30 を、図 1 に示すメタサーバ 76 に対応して、複数のサーバ 72, 73, 74, ……で構成する。そして、図 27 のフローチャートのステップ S705 においては、第 1 端末 20 内において、複数のサーバ 72, 73, 74, ……の数に対応した複数の情報を、複数のサーバ 72, 73, 74, ……に 1:1 にそれぞれ対応した複数の暗号化鍵でそれぞれ暗号化して、複数のサーバ 72, 73, 74, ……の数に対応した複数の暗号化情報  $E_1, E_2, E_3, \dots, E_n$  を生成する。そして、情報処理サーバ（メタサーバ）30 が、複数の暗号化情報  $E_1, E_2, E_3, \dots, E_n$  を受信し、複数のサーバ 72, 73, 74, ……のそれぞ



れで、複数の暗号化情報  $E_1$ ,  $E_2$ ,  $E_3$ ,  $\dots$ ,  $E_n$  を順次復号する。

即ち、第 1 の情報をメタサーバ内の第 1 サーバ 7 2 用の暗号化鍵で暗号化して第 1 の暗号化情報  $E_1$  を生成し、第 2 の情報をメタサーバ内の第 2 サーバ 7 3 用の暗号化鍵で暗号化して第 2 の暗号化情報  $E_2$  を生成し、第 3 の情報をメタサーバ内の第 3 サーバ 7 4 用の暗号化鍵で暗号化して第 3 の暗号化情報  $E_3$  を生成し、 $\dots$ 、第  $n$  の情報をメタサーバ内の第  $n$  サーバ用の暗号化鍵で暗号化して第  $n$  の暗号化情報  $E_n$  を生成し、第 2 レベルの個人情報を生成する。

そして、第 1 の暗号化情報  $E_1$ 、第 2 の暗号化情報  $E_2$ 、第 3 の暗号化情報  $E_3$ 、 $\dots$ 、第  $n$  の暗号化情報  $E_n$  をメタサーバ（情報処理サーバ）3 0 が第 2 レベルの個人情報として受信する。その後、メタサーバ（情報処理サーバ）3 0 の第 1 サーバ 7 2 で、第 1 の暗号化情報  $E_1$  を復号して処理し、第 2 サーバ 7 3 で、第 2 の暗号化情報  $E_2$  を復号して処理し、第 3 サーバ 7 4 で、第 3 の暗号化情報  $E_3$  を復号して処理し、 $\dots$ 、第  $n$  サーバで、第  $n$  の暗号化情報  $E_n$  を復号する。そして、図 2 7 のフローチャートのステップ S 7 0 6、若しくは図 2 8 のステップ S 7 1 7 において、第 2 レベルの個人情報を事業者サーバ（第 2 端末）5 1 に送る。

或いは、第 1 の実施例に係る個人情報保護方式において、図 1、図 2 及び図 3 を参照して説明したように、暗

号化された情報を検索キーとし、その暗号化された検索キー情報から関連づけられる暗号データを検索することが可能なように、暗号化データベースを実現しても良い。

第12の実施例に係る情報処理システムにおいて、情報処理サーバ30にアクションを行う事業者サーバへ送信するための情報を受け渡す際に、第1の実施例及び第1の実施例に係る個人情報保護方式を用いることにより、情報処理サーバ30では、他のサーバと結託しキーを入手しない限り、その情報の中身を見ることが不可能であり、情報処理サーバ30で誰が何をしようとしたのか知ることとはできない。つまり、内部のサーバ管理者でさえ情報が漏れない仕組みとなる。

更に、情報処理サーバ30側に第1の実施例に係る個人情報保護方式を採用し、携帯情報端末20に「エンクリプティッド・ランダムナンバー・メタデータベースシステム」を採用することにより、情報が外部からの攻撃だけでなく、内部の人でさえ、不当に漏れない認証代行モデルとなる。

更に、情報処理サーバ30側に第2～6の実施例に係る種々の個人情報保護方式を採用することにより、情報が外部からの攻撃だけでなく、内部の人でさえ、不当に漏れない認証代行モデルが実現できる。

<第12の実施例の第1変形例：チケットシステム>

イベント会場への第12の実施例の応用を考えてみる。

まず、図 27 のフローチャートに示したように、携帯情報端末 20 を利用し、ステップ S 701 において紙誌面、パーソナルコンピュータ、WEB サイトなどから、興行（日時、座席、会場など）の選択し、その画像コードを撮り、情報処理サーバ 30 に送信する。そして、ステップ S 702 及びステップ S 703 を経て、ステップ S 704 において、情報処理サーバ 30 が携帯情報端末 20 に整理券情報を発行する。その後、ステップ S 705 及びステップ S 706 を経て、チケットの予約・決済がされる。そして、イベント会場入り口では、入場管理者が、携帯情報端末 20 のチケット認証画像コードを読み、サーバで支払い証明を確認し、支払済みであれば、「特定の画像」（OK など）を表示し、管理者が視認し、入場させる。しかしながら、イベント会場入り口での「入場」の操作において時間がかかると、入場が混雑することが考えられる。又、混雑を回避するために、前もってチケット認証画像コード読ませると、前もって読んで特定の画像を得たユーザが他のユーザに携帯経由で転送することが可能なため、入場における認証として役割を果たさない。

この問題点を解決するため、第 12 の実施例の変形例に係るチケットシステムは、図 29 のフローチャートに示す方法を採用する：

（a）まず、ステップ S 761 において、チケット認証カードを印刷した印刷物を複数個用意する。「印刷物」

は、適当な大きさのカードのようなもので良く、画像コードの下に、固有番号が視認可能な形で印刷されている。例えば、2 A 8 4 R T 4 などの固有番号が、画像コードの下に印刷されている。この画像コードは、例えば、QRコードと呼ばれるマトリクス型の二次元コードと、この二次元コードの周囲を取り囲む情報コードとで構成しても良い。以下において、画像コードと番号をセットで印刷したカードを「チケット認証カード」と呼ぶ。なお、画像コードの下に印刷されている固有番号は、認証画像コード内にも埋め込まれている。

(b) そして、ステップ S 7 6 2 において、チケット認証カードに含まれる画像コードを携帯情報端末 2 0 で撮影する。更に、ステップ S 7 6 3 において、携帯情報端末 2 0 から画像コードの情報と第 1 レベルの個人情報の統合情報を情報処理サーバ 3 0 に送信する。

(c) このため、ステップ S 7 6 4 において、情報処理サーバ 3 0 は携帯情報端末 2 0 からのアクション要求を受ける。次に、ステップ S 7 6 5 において、情報処理サーバ 3 0 は事業者サーバ 5 1 の認証と、個人・端末認証をする。ステップ S 7 6 5 において、事業者サーバ 5 1 の認証と携帯情報端末 2 0 の認証ができたら、情報処理サーバ 3 0 は携帯情報端末 2 0 に整理券情報を発行する。

(d) 携帯情報端末 2 0 は、整理券情報を受信するとステップ S 7 6 6 において、チケット認証カードに含ま

れる画像コードの情報と第2レベルの個人情報の統合情報を事業者サーバ51に送信する。ステップS767では、事業者サーバ51において、携帯情報端末20の予約、支払の確認をする。

(e) ステップS768において、事業者サーバ51が、その固有番号を携帯情報端末20に送信する。

(f) イベント会場入り口では、入場管理者は、ステップS769において、携帯情報端末20に表示された固有番号と、チケット認証カードに印刷された視認番号が一致していることを確認する。これは、「チケットを切る」のと同程度の時間で処理可能である。又、チケット認証カードは、印刷ベースで何枚でも発行可能である。又回収後、使いまわすことができる。

以上のように、第12の実施例の変形例に係るチケットシステムによれば、専用読取装置なしで、電子チケットの発行が可能となり、チケットを切るのと同程度の時間（視認のみ）で、入場管理が可能である。

#### < 第12の実施例の第2変形例：口座ロック決済 >

第12の実施例に係る情報処理方法は、印刷物やパーソナルコンピュータ画面上にある画像コードを撮影するだけで、買い物から、代金の支払、つまり決済までを行うシステムの実現に応用できる特徴を有する。金融機関の決済における認証は、大きくは、図30に示したプロセスから実現される。

(a) ステップ S 8 0 1 において、携帯情報端末 2 0 は、画像コードを読んで情報処理サーバ 3 0 に決済を要求する。

(b) 情報処理サーバ 3 0 は携帯情報端末 2 0 からの決済の要求を受けると、ステップ S 8 0 2 において、事業者サーバ 5 1 の認証と、個人・端末認証をし、認証ができたなら、携帯情報端末 2 0 に整理券情報を発行する。

(c) 整理券情報を受けた携帯情報端末 2 0 は、ステップ S 8 0 3 において、再度、情報処理サーバ 3 0 に決済を要求する。

(d) そして、情報処理サーバ 3 0 は、ステップ S 8 0 4 において、事業者サーバ (金融機関) 5 1 に決済を要求する。事業者サーバ (金融機関) 5 1 は、携帯情報端末 2 0 のユーザの対応口座の残金を確認し、ステップ S 8 0 5 において携帯情報端末 2 0 に決済の承認をする。

(e) 決済の承認がされれば、携帯情報端末 2 0 のユーザは、対応口座から所望の金額の引き落としをする。

しかしながら、図 3 0 に示したプロセスでは、ステップ S 8 0 4 ~ ステップ S 8 0 5 の操作の間にタイムラグが発生し、ステップ S 8 0 5 がステップ S 8 0 7 の後になれば、そのタイムラグの間に、ステップ S 8 0 7 の他の事業者 5 2 が対応口座から残金を先に引き落とす。こうなれば、ステップ S 8 0 5 の引き落としが不可能になる可能性がある。

この問題点を解決するため、第 1 2 の実施例の第 2 変

形例では、図 3 1 に示すように、ステップ S 8 1 4 において、口座ロック整理券を発行する。即ち、ステップ S 8 1 4 において、情報処理サーバ 3 0 から事業者サーバ（金融機関）5 1 に対して口座ロック整理券を発行して、口座ロック整理券に対応する携帯情報端末 2 0 の操作が終了するまで、その口座をロックする方式である。

図 3 1 を用いて、本発明の第 1 2 の実施例の第 2 変形例に係る金融機関決済方法を説明する：

（a）ステップ S 8 1 1 ～ S 8 1 3 までは、図 3 0 のステップ S 8 0 1 ～ S 8 0 3 と同様である。ステップ S 8 1 4 の残金確認時に、情報処理サーバ 3 0 から、事業者サーバ（金融機関）5 1 に対して口座ロック整理券を発行する。

（b）口座ロック整理券を発行されると、事業者サーバ（金融機関）5 1 は、携帯情報端末 2 0 のユーザからの引き落としまでの間、事業者サーバ（金融機関）5 1 の対応口座から引き落としが行われないよう対応口座をロックする。

（c）そして、パスポート（口座ロック整理券）に対応する I D を持つユーザからの決済が行われたら、事業者サーバ（金融機関）5 1 の口座を開放する。

< 第 1 2 の実施例の第 3 変形例：デポジット方式決済 >

図 3 0 に示したように、ステップ S 8 0 4 ～ ステップ S 8 0 5 の操作の間にタイムラグが発生し、そのタイム

ラグの間に、他の事業者 52 が対応口座から残金を先に引き落とすことにより、ステップ S 8 0 5 の引き落としが不可能になることを防止するためには、図 3 2 に示すように、これは、情報処理サーバ 3 0 による決済のための一定額をとっておき、そこから引き落とすことにより、他の事業者 52 から起こったステップ S 8 2 7 ~ S 8 2 8 の操作に影響させないにできる：

(a) ステップ S 8 2 1 ~ S 8 2 3 までは、図 3 0 のステップ S 8 0 1 ~ S 8 0 3 と同様である。しかし、15 の実施例の第 3 変形例に係るデポジット方式では、あらかじめ事業者サーバ(金融機関) 5 1 の対応口座から、一定額を引き出しデポジットしておく。デポジットは、情報処理サーバ 3 0 によるサービスに一意に対応しており、同時に複数の決済行為、割り込みが発生することはないように設定されている。

(b) このため、情報処理サーバ 3 0 は、ステップ S 8 2 4 において、事業者サーバ(金融機関) 5 1 に決済を要求すると、事業者サーバ(金融機関) 5 1 は、携帯情報端末 2 0 のユーザの対応口座の専用デポジットの方の残金を確認し、ステップ S 8 2 5 において携帯情報端末 2 0 に決済の承認をする。

(c) 決済の承認がされれば、携帯情報端末 2 0 のユーザは、対応口座の専用デポジットから所望の金額の引き落としをする。



(第13の実施例)

図33は、インターネット（通信ネットワーク）70に接続される一般通信端末（主第1端末）20n、カメラ付き携帯情報端末（補助第1端末）20m、事業者サーバ（第2端末）51及び情報処理サーバ30に着目した本発明の第13の実施例に係る情報処理システムの構成図である。

ここで、カメラ付き携帯情報端末（補助第1端末）20mとは、第12の実施例に係る情報処理システムで説明したと同様な、画像コード読取装置19を備えた携帯情報端末である。画像コード読取装置19には、カメラ、赤外線スキャナなど各種スキャナ等が含まれる。「画像コード」には、第1～第12の実施例と同様に、一次元コード、二次元コード、ウォーターマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等が含まれうる。図33に示すように、カメラ付き携帯情報端末（補助第1端末）20mは、画像コード読取装置19の他、処理制御装置21、画像表示装置15、画像データ記憶装置12、個人情報記憶装置18とを備えている。そして、処理制御装置21は、画像取込手段（モジュール）11と、画像コード解読手段（モジュール）13と、画像コード変換手段（モジュール）14と、統合データ編集手段（モジュール）16と、電話機能制御手段（モジュール）17とを有す

る処理制御装置 21 を備えている。一方、一般通信端末（主第 1 端末）20n は、画像コード読取装置 19 を備えないパーソナルコンピュータ等の通信端末を意味する。

現実には、インターネット（通信ネットワーク）70 には、複数の事業者サーバ（第 2 端末）51、複数のカメラ付き携帯情報端末（補助第 1 端末）20m、複数の一般通信端末（主第 1 端末）20n が接続されうるが、説明を簡単にするために、単一の事業者サーバ（第 2 端末）51 と、単一のカメラ付き携帯情報端末（補助第 1 端末）20m 及び単一の一般通信端末（主第 1 端末）20n を図示している。実際には、カメラ付き携帯情報端末（補助第 1 端末）20m は、デジタル通信網（他の通信ネットワーク）に接続され、このデジタル通信網が中継処理装置を介して、インターネット（通信ネットワーク）70 に接続される構成で構わない。

図 33 に示した情報処理サーバ 30 は、画像コード画面送信手段（モジュール）331 と、統合情報受信手段（モジュール）332 と、携帯情報端末認証手段（モジュール）333 と、要求画面送信手段（モジュール）334 と、アクション実行手段（モジュール）335 を有する CPU 320 を備える。更に、この CPU 320 には、事業者情報登録装置 37 と個人情報登録装置 38 が接続されている。

ここで、画像コード画面送信手段（モジュール）33

1 は、画像コードを含む画面の送信をする論理回路である。「画像コード」の内容には、一意に特定できる乱数（ワンタイムパスワードのようなもの）とタイムスタンプが格納されている。又、統合情報受信手段（モジュール）332 は、カメラ付き携帯情報端末（補助第1端末）20mからの、画像コードの内容と個人情報との統合情報の受信をする論理回路で、携帯情報端末認証手段（モジュール）333 は、カメラ付き携帯情報端末（補助第1端末）20mの認証をする論理回路で、要求画面送信手段（モジュール）334 は、カメラ付き携帯情報端末（補助第1端末）20mに要求された画面を送信する論理回路で、アクション実行手段（モジュール）335 は、カメラ付き携帯情報端末（補助第1端末）20mに対しアクションの実行をする論理回路である。

更に、第12の実施例に係る情報処理システムと同様に、事業者情報登録装置37は、事業者情報を記憶する記憶装置で、個人情報登録装置38は、認証対象となる個人情報記憶する記憶装置である。

図34のフローチャートを用いて、本発明の第13の実施例に係る情報処理方法を説明する：

（a）まず、ステップS721で、一般通信端末（主第1端末）20nの画面を見ているユーザは、画面上のインターフェースとして用意されている「画像コードの表示」ボタンをクリックし、情報処理サーバ30に画像

コードの表示を要求する。

(b) すると、情報処理サーバ 30 は、ステップ S 7 2 2 において、画像コードを含む画面を一般通信端末(主第 1 端末) 20 n に送信する。そして、ステップ S 7 2 3 において、ユーザは、一般通信端末(主第 1 端末) 20 n の画面に表示された画像コードをカメラ付き携帯情報端末(補助第 1 端末) 20 m で読み取る。これによりカメラ付き携帯情報端末(補助第 1 端末) 20 m の統合データ編集手段(モジュール) 16 は、一般通信端末(主第 1 端末) 20 n の画面に表示された画像コードの内容(乱数+タイムスタンプ)とカメラ付き携帯情報端末(補助第 1 端末) 20 m 内の情報(個人認証 ID(固定乱数))を統合した情報を編集し、統合情報を作成する。そして、カメラ付き携帯情報端末(補助第 1 端末) 20 m は、統合データ編集手段(モジュール) 16 が編集した統合情報を、情報処理サーバ 30 に送信する。

(c) ステップ S 7 2 4 において、情報処理サーバ 30 は、受信した統合情報と個人情報登録装置 38 に格納されている情報を対照し、ユーザの認証を行う。但し、ステップ S 7 2 2 においてタイムスタンプ情報を送付した時刻から時間があまりにも経っているものステップ S 7 2 4 では認証しない。

(d) ステップ S 7 2 4 においてユーザの認証できれば、ステップ S 7 2 5 において情報処理サーバ 30 は、ユーザが求める画面を一般通信端末(主第 1 端末) 20

n に送信し、一般通信端末（主第 1 端末）20n の画面に表示する。或いは、ステップ S 7 2 5 において情報処理サーバ 30 は、ユーザが求めるアクションの実行をする。ステップ S 7 2 3、ステップ S 7 2 4 が完了して認証しない限り、ステップ S 7 2 5 に遷移しない。

図 3 5 は、第 1 3 の実施例に係る情報処理方法の実施に用いる情報処理サーバ 30 の動作を説明するフローチャートである。

（a）一般通信端末（主第 1 端末）20n から、情報処理サーバ 30 に画像コードの表示の要求があると、情報処理サーバ 30 の画像コード画面送信手段（モジュール）331 は、ステップ S 7 3 1 において、画像コードを含む画面を一般通信端末（主第 1 端末）20n に送信する。

（b）情報処理サーバ 30 の統合情報受信手段（モジュール）332 は、ステップ S 7 3 2 において、カメラ付き携帯情報端末（補助第 1 端末）20m からの、画像コードの内容と個人情報との統合情報の受信をする。

（c）情報処理サーバ 30 の携帯情報端末認証手段（モジュール）333 は、ステップ S 7 3 3 において、受信した統合情報と個人情報登録装置 38 に格納されている情報を対照し、カメラ付き携帯情報端末（補助第 1 端末）20m の認証をする。

（d）ステップ S 7 3 3 においてユーザの認証できれ

ば、情報処理サーバ30の要求画面送信手段（モジュール）334は、ステップS734において、カメラ付き携帯情報端末（補助第1端末）20mに要求された画面を送信する。又は、情報処理サーバ30のアクション実行手段（モジュール）335は、ステップS734において、カメラ付き携帯情報端末（補助第1端末）20mから要求されたアクションの実行をする。ステップS733においてユーザの認証できなければ、処理を終了する。

図33には、インターネット（通信ネットワーク）70に、事業者サーバ51、情報処理サーバ30、カメラ付き携帯情報端末20m及び一般通信端末20nが接続された情報処理システムの構成図を示した。この場合、一般通信端末20nを事業者が提供するサービス専用の端末（以下、「サービス専用端末20n」と言う。）とすれば、このサービス専用端末20nを介するサービスにも適用できる。サービス専用端末20nとして好適な例としては、コンビニに設置された端末などがある。サービス専用端末20nにおけるサービスがユーザの住所や名前などは必要な場合、図34及び図35のフローチャートと同様な手順で、ユーザの認証をすることにより、そのユーザの情報を安全に獲得できる。更に、ユーザはそのサービス専用端末20nに個人情報を入力する手間が省け、サービス専用端末20nに表示された画像コー

ドを読むだけで済む。

又、第 13 の実施例に係る情報処理方法と第 1 ～ 第 6 の実施例で説明した個人情報保護方式とを組み合わせることが可能である。

又、第 13 の実施例に係る情報処理方法において、パーソナルコンピュータなどの一般通信端末 20 n のディスプレイ上に、メニュー・表などの形式でアイテムを表示しておき、或いは検索結果を表示し、それらに画像コード生成のリンクを貼っておくようにしても良い。この様にしておけば、その検索結果をダイナミックに光学読み取り可能な形式で画像コード化して表示することができる。の一般通信端末 20 n のディスプレイ上に表示されるこれらの画像コードは、偽造改竄が不能である。このような構成にしておけば、発行事業者が認証可能で、画像コードは、携帯情報端末 20 で読み取り可能で、携帯情報端末 20 によって、個人認証が可能となる（会員認証、決済系の認証が可能である。）。そして、携帯情報端末 20 の個人情報記憶装置に格納された個人認証識別情報から、それに連結されているサーバなどから、個人情報を紐付けして取り出すことができない（名寄せできない。）という利点を有する。

この様に、第 13 の実施例に係る情報処理方法によれば、全てのランザクション、決裁・決済行為が、検索機能、選択機能、編集統合機能と連動することにより、ダイナミックに可能となる。例えば、インテリアを、テ

ーブルと椅子とライトを選択した場合、それらのセットを統合し、コード生成すれば、一発で発注完了することがある。

つまり、第 1 3 の実施例に係る情報処理方法によれば、あらゆる通販・物販で選択済みのアイテムを一括発注できる。又、第 1 3 の実施例に係る情報処理方法によれば、必要なセキュリティレベルに応じた長さのワンタイムパスワードなどをコード生成時に埋め込めばセキュリティ精度が任意にコントロールできる。

#### (第 1 4 の実施例)

第 1 4 の実施例に係る情報処理方法は、第 1 携帯情報端末 2 0 p 及び第 2 携帯情報端末 2 0 q 間のデータのやり取りにおける認証代行方式である。これは、異種機種である第 1 携帯情報端末 2 0 p と第 2 携帯情報端末 2 0 q 間のデータ処理を行う際にメタサーバ（情報処理サーバ）3 0 を介することにより異種機種間の記述方式の違いを回避して、データの処理を安全に可能とする方式である。

図 3 6 は、インターネット（通信ネットワーク）7 0 に接続される事業者サーバ 5 1、情報処理サーバ 3 0、第 1 携帯情報端末 2 0 p 及び第 2 携帯情報端末 2 0 q に着目した、本発明の第 1 4 の実施例に係る情報処理システムの構成図である。ここで、第 1 携帯情報端末 2 0 p



及び第2携帯情報端末20qは、それぞれ第12の実施例に係る情報処理システムで説明したと同様な、画像コード読取装置19p及び19qを備えた携帯情報端末である。画像コード読取装置19p及び19qには、既に説明したように、カメラ、赤外線スキャナなど各種スキャナが含まれうる。「画像コード」も、第1～第13の実施例での説明と同様な、一次元コード、二次元コード、ホログラムコード、ウォータマーク（すかし技術）、ステガノグラフィー（画像への情報埋め込み）や、種々の他の自動認識コード等を含み得るものである。

図3.6に示すように、第1携帯情報端末20pは、画像コード読取装置19pの他、処理制御装置21p、画像表示装置15p、画像データ記憶装置12p、個人情報記憶装置18pとを備えている。そして、処理制御装置21pは、画像取込手段（モジュール）11pと、画像コード解読手段（モジュール）13pと、画像コード変換手段（モジュール）14pと、統合データ編集手段（モジュール）16pと、電話機能制御手段（モジュール）17pとを有する処理制御装置21pを備えている。

一方、第2携帯情報端末20qは、画像コード読取装置19qの他、処理制御装置21q、画像表示装置15q、画像データ記憶装置12q、個人情報記憶装置18qとを備えている。そして、処理制御装置21qは、画像取込手段（モジュール）11qと、画像コード解読手段（モジュール）13qと、画像コード変換手段（モジ

ュール) 14 q と、統合データ編集手段 (モジュール) 16 q と、電話機能制御手段 (モジュール) 17 q とを有する処理制御装置 21 q を備えている。現実には、インターネット (通信ネットワーク) 70 には、複数の事業者サーバ 51、複数の携帯情報端末 20 p, 20 q, ……が接続されうるが、説明を簡単にするために、単一の事業者サーバ 51 と、第1携帯情報端末 20 p 及び携帯情報端末 20 q を図示している。実際には、第1携帯情報端末 20 p 及び第2携帯情報端末 20 q は、それぞれ、デジタル通信網 (他の通信ネットワーク) に接続され、このデジタル通信網が中継処理装置を介して、インターネット (通信ネットワーク) 70 に接続される構成で構わない。

図 3.6 に示した情報処理サーバ 30 は、第1携帯情報端末情報獲得手段 (モジュール) 341 と、認証用画像コード生成手段 (モジュール) 342 と、画像データ送信手段 (モジュール) 343 と、第2携帯情報端末情報獲得手段 (モジュール) 344 と、情報編集手段 (モジュール) 345 と、編集情報送信手段 (モジュール) 346 とを備える。

更に、この CPU 320 には、事業者情報登録装置 37 と個人情報登録装置 38 が接続されている。

ここで、第1携帯情報端末情報獲得手段 (モジュール) 341 は、第1携帯情報端末 20 p からの情報の獲得を

する論理回路である。又、認証用画像コード生成手段（モジュール）342は、認証用画像コードの生成をする論理回路である。更に、画像データ送信手段（モジュール）343は、認証用画像コードを画像データとして第1携帯情報端末20pに送信する論理回路であり、第2携帯情報端末情報獲得手段（モジュール）344は、第2携帯情報端末20qからの認証用画像コード内の情報と第2携帯情報端末20qの機体情報の受信をする論理回路であり、情報編集手段（モジュール）345は、第2携帯情報端末20qの機体情報による第1携帯情報端末20pの情報の編集をする論理回路である。そして、編集情報送信手段（モジュール）346は、第2携帯情報端末20qに第1携帯情報端末20pの情報を送信する論理回路である。又、第12の実施例に係る情報処理システムと同様に、事業者情報登録装置37は、事業者情報を記憶する記憶装置で、個人情報登録装置38は、認証対象となる個人情報記憶する記憶装置である。

図37のフローチャートを用いて、本発明の第14の実施例に係る情報処理方法を説明する。ここでは第1携帯情報端末20pから第2携帯情報端末20qにデータを受け渡す場合の流れを仮定する：

（a）まず、ステップS741において、紙媒体等に印刷された事業用画像コードを第1携帯情報端末20pの画像コード読取装置19pが撮影し、画像データ記憶

装置 1 2 p に格納する。第 1 携帯情報端末 2 0 p の画像取込手段（モジュール）1 1 p は、画像データ記憶装置 1 2 p から事業用画像コードを取り込み、この事業用画像コードに含まれる情報を画像コード解読手段（モジュール）1 3 q により解読し、解読された情報と個人情報記憶装置 1 8 p に記憶された個人情報とを統合データ編集手段（モジュール）1 6 p が編集統合し、第 1 統合情報を作成する。そして、第 1 携帯情報端末 2 0 p は、この第 1 統合情報を、仲介サーバである情報処理サーバ 3 0 に送信する。

（b）ステップ S 7 4 2 においては、情報処理サーバ 3 0 が第 1 携帯情報端末 2 0 p からの第 1 統合情報を獲得し、認証用画像コードを生成し、画像データとして第 1 携帯情報端末 2 0 p に送信する。すると、ステップ S 7 4 3 において、第 1 携帯情報端末 2 0 p の画像表示装置 1 5 p の画面上に認証用画像コードが表示される。

（c）ステップ S 7 4 4 において、第 1 携帯情報端末 2 0 p の画像表示装置 1 5 p に表示された認証用画像コードを第 2 携帯情報端末 2 0 q の画像コード読取装置 1 9 q が撮影し、これを画像データ記憶装置 1 2 q に格納する。第 2 携帯情報端末 2 0 q の画像取込手段（モジュール）1 1 q は、画像データ記憶装置 1 2 q から認証用画像コードを取り込み、この認証用画像コードに含まれる情報を画像コード解読手段（モジュール）1 3 q により解読し、解読された情報と個人情報記憶装置 1 8 q に

記憶された機体情報とを統合データ編集手段（モジュール）16qが編集統合し、第2統合情報を作成する。

（d）ステップS745においては、第2携帯情報端末20qから情報処理サーバ30へ第2統合情報が送信される。ステップS746では、情報処理サーバ30において、第2携帯情報端末20qの機体情報を用い、第1携帯情報端末20pの情報を整え、第2携帯情報端末20qに送信する。即ち、第2携帯情報端末20qに第1携帯情報端末20pからの情報を送信する。

図38は、第14の実施例に係る情報処理方法の実施に用いる情報処理サーバ30の動作を説明するフローチャートである：

（a）第1携帯情報端末20pがこの第1統合情報を情報処理サーバ30に送信すると、ステップS751において、情報処理サーバ30の第1携帯情報端末情報獲得手段（モジュール）341が、第1携帯情報端末20pからの第1統合情報の獲得をする。

（b）次に、ステップS752において、情報処理サーバ30の認証用画像コード生成手段（モジュール）342は、認証用画像コードの生成をする。

（c）そして、ステップS753において、情報処理サーバ30の画像データ送信手段（モジュール）343は、認証用画像コードを画像データとして第1携帯情報端末20pに送信する。

(d) 第1携帯情報端末20pに表示された認証用画像コードを第2携帯情報端末20qが撮影し、第2携帯情報端末20qから情報処理サーバ30へ第2統合情報が送信されるト、ステップS754において、情報処理サーバ30の第2携帯情報端末情報獲得手段(モジュール)344が、第2携帯情報端末20qからの第2統合情報に含まれる認証用画像コード内の情報と第2携帯情報端末20qの機体情報の受信をする。

(e) その後、ステップS755において、情報処理サーバ30の情報編集手段(モジュール)345は、第2携帯情報端末20qの機体情報による第1携帯情報端末20pの情報の編集をする。

(f) 次に、ステップS756において、情報処理サーバ30の編集情報送信手段(モジュール)346は、第2携帯情報端末20qに第1携帯情報端末20pの情報を送信する。

#### <第14の実施例の第1変形例：特定情報交換>

図39に示す方式で第1携帯情報端末20sの特定情報を第2携帯情報端末20tの携帯電話の取得する：

(a) まず、ステップS901において、紙媒体等に印刷された事業用画像コードを第1携帯情報端末20sの画像コード読取装置が撮影し、画像データ記憶装置に格納する。第1携帯情報端末20sの画像取込手段(モジュール)は、画像データ記憶装置から事業用画像コー

ドを取り込み、この事業用画像コードに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された情報と個人情報記憶装置に記憶された個人情報とを統合データ編集手段（モジュール）が編集統合し、第1統合情報を作成する。第1統合情報には、第1携帯情報端末20sから第2携帯情報端末20tに登録させた特定情報も含ませる。そして、ステップS902において、第1携帯情報端末20sは、この第1統合情報を、仲介サーバである情報処理サーバ30に送信する。

（b）ステップS903において、情報処理サーバ30が第1携帯情報端末20sからの第1統合情報を獲得し、特定情報（例えば電話帳登録情報）を画像コードに生成する。ステップS904において特定情報の画像コードを、画像データとして第1携帯情報端末20sに送信する。すると、ステップS905において、第1携帯情報端末20sの画像表示装置の画面上に特定情報の画像データが表示される。

（c）ステップS905において、第1携帯情報端末20sの画像表示装置に表示された特定情報の画像データ（電話帳登録情報）を第2携帯情報端末20tの画像コード読取装置が撮影し、これを画像データ記憶装置に格納する。第2携帯情報端末20tの画像取込手段（モジュール）は、画像データ記憶装置から特定情報の画像データ（電話帳登録情報）を取り込み、この特定情報の画像データ（電話帳登録情報）に含まれる情報を画像コ

ード解読手段（モジュール）により解読し、解読された特定情報と個人情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第2統合情報を作成する。

（d）ステップS906においては、第2携帯情報端末20tから情報処理サーバ30へ第2統合情報が送信される。ステップS907では、情報処理サーバ30において、第2携帯情報端末20tの機体情報を用い、第1携帯情報端末20sの特定情報（電話帳登録情報）を整え、ステップS908において第2携帯情報端末20tに送信する。即ち、第2携帯情報端末20tに第1携帯情報端末20sからの特定情報（電話帳登録情報）をステップS908において送信する。場合によってはパーソナルコンピュータ20zなどの別機体に第1携帯情報端末20sからの特定情報（電話帳登録情報）を同時送信しても良い。

なお、必要であれば、第2携帯情報端末20tの特定情報の画像コードを発行し第1携帯情報端末20sの携帯電話で読ませることで情報交換させる（手順は同じだが、相手の携帯機種が分かっているので、相手の携帯電話用の画像コードを作成し表示して読ませれば良い）。

< 第14の実施例の第2変形例：所有者の相性占い >

二次元コードの情報（アクション情報），第1携帯情報端末20sの情報（個人情報），第2携帯情報端末2



0 t の情報（個人情報）に起因したアクションを実現できる。つまり、2つ以上の個人情報によるアクションが実現できる。例えば、第1携帯情報端末20sの所有者と第2携帯情報端末20tの所有者の相性占いなどが挙げられる。図40は、第1携帯情報端末20sの所有者と第2携帯情報端末20tの所有者の相性占いを想定している：

（a）まず、ステップS911において、紙媒体等に印刷された相性占いコードを第1携帯情報端末20sの画像コード読取装置が撮影し、画像データ記憶装置に格納する。第1携帯情報端末20sの画像取込手段（モジュール）は、画像データ記憶装置から相性占いコードを取り込み、この相性占いコードに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された情報と個人情報記憶装置に記憶された個人情報とを統合データ編集手段（モジュール）が編集統合し、第1統合情報を作成する。第1統合情報には、第1携帯情報端末20sから第2携帯情報端末20tに登録させたいアクション情報も含ませる。そして、ステップS912において、第1携帯情報端末20sは、この第1統合情報を、仲介サーバである情報処理サーバ30に送信する。

（b）ステップS913において、情報処理サーバ30が第1携帯情報端末20sからの第1統合情報を獲得し、アクション情報を画像コードに生成する。ステップS914においてアクション情報（第2携帯情報端末2

0 t に読ませたい占い情報) の画像コードを、画像データとして第 1 携帯情報端末 20 s に送信する。すると、ステップ S 9 1 5 において、第 1 携帯情報端末 20 s の画像表示装置の画面上にアクション情報の画像データが表示される。

(c) ステップ S 9 1 5 において、第 1 携帯情報端末 20 s の画像表示装置に表示されたアクション情報の画像データを第 2 携帯情報端末 20 t の画像コード読取装置が撮影し、これを画像データ記憶装置に格納する。第 2 携帯情報端末 20 t の画像取込手段(モジュール)は、画像データ記憶装置からアクション情報の画像データを取り込み、このアクション情報の画像データに含まれる情報を画像コード解読手段(モジュール)により解読し、解読されたアクション情報と個人情報記憶装置に記憶された機体情報とを統合データ編集手段(モジュール)が編集統合し、第 2 統合情報を作成する。

(d) ステップ S 9 1 6 においては、第 2 携帯情報端末 20 t から情報処理サーバ 30 へ第 2 統合情報が送信される。ステップ S 9 1 7 では、情報処理サーバ 30 において、第 2 携帯情報端末 20 t の機体情報を用い、第 1 携帯情報端末 20 s のアクション情報を整え、第 1 携帯情報端末 20 s の所有者と第 2 携帯情報端末 20 t の所有者の相性占いを行う。ステップ S 9 1 8 において、第 1 携帯情報端末 20 s の所有者と第 2 携帯情報端末 20 t の所有者の相性占いの結果は、第 2 携帯情報端末 2

0 t に送信される。場合によってはパーソナルコンピュータ 20 z などの別機体に第 1 携帯情報端末 20 s からの第 1 携帯情報端末 20 s の所有者と第 2 携帯情報端末 20 t の所有者の相性占いの結果を同時送信しても良い。

< 第 14 の実施例の第 3 変形例：パーミッション機能を伴う情報共有 >

複数、即ち、第 1 携帯情報端末 20 s、第 2 携帯情報端末 20 t、第 3 携帯情報端末 20 u、第 4 携帯情報端末 20 v の 4 台の端末があるとする。この 4 台の端末中の第 1 携帯情報端末 20 s、第 2 携帯情報端末 20 t 及び第 4 携帯情報端末 20 v の 3 台の端末のみ情報が共有され、第 3 携帯情報端末 20 u には情報が共有できないように、パーミッション機能を設定して特定の端末にのみ情報が共有されるようにするシステムである。

(a) まず、情報処理サーバ 30 において、第 1 携帯情報端末 20 s からアクションがあつとき、第 2 携帯情報端末 20 t 及び第 4 携帯情報端末 20 v のみにそのアクションを許可するように設定しておく。

(b) 次に、ステップ S 9 2 1 において、第 1 携帯情報端末 20 s の画像表示装置に表示された特定の情報の画像データを第 2 携帯情報端末 20 t の画像コード読取装置が撮影し、この特定の情報の画像データに含まれる情報を画像コード解読手段(モジュール)により解読し、解読された特定の情報と第 2 携帯情報端末 20 t の個人

情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第2携帯情報端末20tの統合情報を作成する。そして、第2携帯情報端末20tから第2携帯情報端末20tの統合情報を情報処理サーバ30へ送信する。

（c）情報処理サーバ30において、第2携帯情報端末20tに対してアクションが許可されているのを確認し、第2携帯情報端末20tの機体情報を用い、第1携帯情報端末20sの特定の情報を整える。そして、ステップS922において、第1携帯情報端末20pから得られた特定の情報は、第2携帯情報端末20tに第2携帯情報端末20tの機体に合致した形式で、送信される。

（d）次に、ステップS923において、第1携帯情報端末20sの画像表示装置に表示された特定の情報の画像データを第3携帯情報端末20uの画像コード読取装置が撮影し、この特定の情報の画像データに含まれる情報を画像コード解読手段（モジュール）により解読し、解読された特定の情報と第3携帯情報端末20uの個人情報記憶装置に記憶された機体情報とを統合データ編集手段（モジュール）が編集統合し、第3携帯情報端末20uの統合情報を作成する。そして、第3携帯情報端末20uから第3携帯情報端末20uの統合情報を情報処理サーバ30へ送信したとする。

（e）しかし、情報処理サーバ30においては、第3携帯情報端末20uに対してアクションが許可されてい

ないので、第3携帯情報端末20uの機体情報を用い、第1携帯情報端末20sの特定の情報を整えることができない。このため、ステップS924において、第1携帯情報端末20pから得られた特定の情報は、第3携帯情報端末20uに送信できず、エラーが送信される。

(f) 更に、第1携帯情報端末20sの画像表示装置に表示された特定の情報の画像データを第4携帯情報端末20vの画像コード読取装置が撮影し、解読された特定の情報と第4携帯情報端末20vの個人情報記憶装置に記憶された機体情報との統合情報が作成され、情報処理サーバ30へ送信されれば、情報処理サーバ30においては、第4携帯情報端末20vに対してアクションが許可されているのを確認し、第4携帯情報端末20vの機体情報を用い、第1携帯情報端末20sの特定の情報を整えることができる。そして、その後、第1携帯情報端末20pから得られた特定の情報は、第4携帯情報端末20vに第4携帯情報端末20vの機体に合致した形式で送信される。

この様にして、第1携帯情報端末20sの特定の情報のみが、第2携帯情報端末20t及び第4携帯情報端末20vに送られ、第3携帯情報端末20uには送信できなくなる。情報が共有できないように、パーミッション機能を設定して特定の端末にのみ情報が共有されるようにするシステムである

第14の実施例の第3変形例に係る情報処理システム

のパーミッション機能は、タイムスタンプによって設定しても良い。更に、も考えられる。なお、第14の実施例の第3変形例に係る情報処理システムは、自作の着メロ交換など携帯情報端末によって依存するものに効果的である。

<第14の実施例の第4変形例：コンテンツ同期方式>

2台以上の携帯情報端末（携帯電話）で、違うコンテンツ、例えば音声・音楽ファイルをダウンロードし、同時に再生を行うことによって、BGMと朗読、伴奏と主旋律、JAMセッションなどを実現する。このとき、JAMセッションなどは、携帯情報端末（携帯電話）の同期が必要になる。

第14の実施例の第4変形例に係る情報処理方法においては、各携帯情報端末（携帯電話）は、絶対時間を持っており、それらは共通化されている。例えば電波時計などで合わせたり、どこかのサーバに時刻情報があつたり、それに同期したクロックを持っている。（或いは、画像コードを読んだとき、クロック（時刻）情報を当該サーバから読込んでも良い。）。各携帯情報端末は、同時演奏マークを読むと、開始タイミングが指定され、ほぼ、同時（1，2秒ずれても良い）に演奏開始すると、先のクロックに同期し同時に演奏が始まる。例えば、最も近い、30秒刻みの、時刻に開始するなど、小節毎に同期を取ることも可能。又、MIDIと連動させても良

い。

(その他の実施例)

上記のように、本発明は第1乃至第14の実施例によって記載したが、この開示の一部をなす論述及び図面はこの発明を限定するものであると理解すべきではない。この開示から当業者には様々な代替実施例及び運用技術が明らかとなろう。

第1～第3の実施例においては、第1のウェアラブルコンピュータ（携帯情報端末）10aから送信元メタデータMD0を発生させる流れを例示したが、事業者サーバ51等側からメタデータを生成してユーザ側に送信されるような逆の流れで個人情報保護方式を利用しても同様のセキュリティを確保することができる。

又、複数のコミュニティに属する場合に、発信者はどのコミュニティに対して送信しているのかを、第1のウェアラブルコンピュータ10aの入力部位から指定したり、SIMカード、ICチップ又はRFID等を差し替えたり、第1のウェアラブルコンピュータ10aによってスキャンするコード等に埋め込んでおいて識別したり様々な方法を選択しても構わない。

第4～第6の実施例においては、第1のウェアラブルコンピュータ10aから送信元メタデータMD0を発生させる流れを例示したが、事業者サーバ51等側からメ

タデータを生成してユーザ側に送信されるような逆の流れで個人情報保護方式を利用しても同様のセキュリティを確保することができる。

又、複数のコミュニティに属する場合に、発信者はどのコミュニティに対して送信しているのかを、第1のウェアラブルコンピュータ10aの入力部位から指定したり、SIMカード、ICチップ又はRFID等を差し替えたり、第1のウェアラブルコンピュータ10aによってスキャンするコード等に埋め込んでおいて識別したり様々な方法を選択しても構わない。

又、第7～第11の実施例で説明した第1のウェアラブルコンピュータ10aで生成された検索タグ情報CODEを用いる暗号化鍵取得方法を、第2の実施例で説明される電子商取引や、第3の実施例で説明されるコミュニティ内の情報交換における情報保護方式に用いることも可能である。

第7～第11の実施例で説明した検索タグ情報CODE2は、暗号化して送信されると説明しているが、暗号化プロトコルSSL等を用いた暗号通信方法を用いる場合は暗号化せずに検索タグ情報CODE2をそのまま送信することが可能である。

例えば、通信端末へ情報を送信すると同時に、パーソナルコンピュータ等の別の機体にも情報を送るように、送信先情報を付加して情報処理サーバ30a、30bに画像を送信することも可能である。



この様に、本発明はここでは記載していない様々な実施例等を含むことは勿論である。したがって、本発明の技術的範囲は上記の説明から妥当な請求の範囲記載に係る発明を特定するために必要と認める事項によってのみ定められるものである。なお、2002年5月31日に出願された特願2002-160369号の開示内容の全体、2002年7月30日に提出された特願2002-222183号の開示内容の全体、2003年8月29日に提出された特願2003-307872号の開示内容の全体、及び2003年9月29日に提出された特願2003-338624号の開示内容の全体は、それぞれ参照により本明細書に挿入されたものとする。

#### 産業上の利用可能性

本発明は、ユビキタス環境下における通信において、個人情報等のデータを当事者以外から秘匿して、種々の電子商取引の分野に適用可能である。更に、イベント会場等の入場管理の分野にも適用できる。

### 請求の範囲

1. 認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理サーバにおいて、

前記認証情報を記憶した認証情報記憶装置と、

前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する認証画像生成モジュールと、

前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を、前記認証端末から取得する認証情報取得モジュールと、

前記認証パラメータ記憶装置を参照して、前記認証情報取得モジュールで取得した前記認証画像の情報が、前記認証画像生成モジュールで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するかどうかを判定し、その結果を前記通信端末に送信する認証情報照合モジュール

とを備えることを特徴とする情報処理サーバ。

2. 前記認証画像生成モジュールで生成する認証パラメータは、一意に特定できる乱数及び日時 of のいずれか1つ以上を含むことを特徴とする請求の範囲第1項に記載

の情報処理サーバ。

3. 前記認証画像生成モジュールにおいて、前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報照合モジュールにおいて、前記認証情報取得モジュールによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求の範囲第1項に記載の情報処理サーバ。

4. 前記認証画像生成モジュールにおいて、第1の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報取得モジュールにおいて、前記第1の通信ネットワークとは異なる第2の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求の範囲第1項に記載の情報処理サーバ。

5. 前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした

情報であることを特徴とする請求の範囲第1項に記載の情報処理サーバ。

6. 前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求の範囲第1項に記載の情報処理サーバ。

7. 前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求の範囲第1項に記載の情報処理サーバ。

8. 前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、  
前記認証画像生成モジュールにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、  
前記認証情報照合モジュールにおいて、前記結果を前記コンテンツ提供サーバに送信する  
ことを特徴とする請求の範囲第1項に記載の情報処理サーバ。

9. 認証端末が備える認証情報を利用して、認証情報を備えない通信端末を認証する情報処理システムに用いられる情報処理方法において、

前記認証情報を認証情報記憶装置に記憶するステップと、

認証画像生成モジュールによって、前記通信端末の認証依頼を受信すると、認証パラメータを生成し、前記認証パラメータを含む認証画像を生成して前記通信端末に送信し、前記認証パラメータを認証パラメータ記憶装置に記憶する前記認証画像を生成するステップと、

認証情報取得モジュールによって、前記認証端末から、前記通信端末から取得した前記認証画像の情報と、前記認証端末が備える前記認証情報を取得するステップと、

認証情報照合モジュールによって、前記認証パラメータ記憶装置を参照して、前記認証画像の情報が、前記認証画像を生成するステップで生成された画像の情報であり、更に、前記認証端末が備える前記認証情報が、前記認証情報記憶装置に記憶した前記認証情報と一致するかどうかを判定し、その結果を前記通信端末に送信する前記認証情報を照合するステップ

とを備えることを特徴とする情報処理方法。

10. 前記認証画像を生成するステップで生成する認証パラメータは、一意に特定できる乱数及び日時のいずれか1つ以上を含むことを特徴とする請求の範囲第9項に記載の情報処理方法。

11. 前記認証画像を生成するステップにおいて、

前記認証パラメータ記憶装置に、前記認証パラメータの有効日時を更に記憶し、

前記認証情報を照合するステップにおいて、前記認証情報を取得するステップによって取得した日時が、前記認証パラメータ記憶装置に記憶された前記認証パラメータの有効日時以前の場合に認証を許可し、前記認証パラメータの有効日時以降の場合に認証を不可にする

ことを特徴とする請求の範囲第9項に記載の情報処理方法。

12. 前記認証画像を生成するステップにおいて、第1の通信ネットワークを利用して前記通信端末に前記認証画像を送信し、

前記認証情報を取得するステップにおいて、前記第1の通信ネットワークとは異なる第2の通信ネットワークを利用して前記認証端末から前記認証画像の情報と前記認証情報を取得する

ことを特徴とする請求の範囲第9に記載の情報処理方法。

13. 前記認証画像の情報は、前記通信端末から取得した前記認証画像を、前記認証端末においてデコードした情報であることを特徴とする請求の範囲第9項に記載の情報処理方法。

14. 前記認証画像の情報は、前記通信端末から取得し、前記認証端末から受信した前記認証画像を、デコードした情報であることを特徴とする請求の範囲第9項に記載の情報処理方法。

15. 前記通信端末から前記認証画像の情報を取得する場合、前記認証端末によって、前記通信端末に提示された認証画像を撮影しデコードすることを特徴とする請求の範囲第9項に記載の情報処理方法。

16. 前記情報処理システムは、前記通信端末にコンテンツを提供するコンテンツ提供サーバを更に備えており、

前記認証画像を生成するステップにおいて、前記コンテンツ提供サーバから、前記通信端末の認証依頼を受信し、

前記認証情報を照合するステップにおいて、前記結果を前記コンテンツ提供サーバに送信する

ことを特徴とする請求の範囲第9項に記載の情報処理方法。

17. 通信端末識別子によって検索される対応情報を格納する識別子対応情報記憶装置と、

通信端末から入力される情報を、前記対応情報に従って変換する情報変換モジュール

とを備えることを特徴とする情報処理サーバ。

18. 前記通信端末から入力される情報から画像を作成する画像作成モジュールを更に備えることを特徴とする請求の範囲第17項項に記載の情報処理サーバ。

19. 前記通信端末が情報交換を許可されているか示す許可情報を格納する許可情報記憶装置と、

前記許可情報を判定する許可判定モジュール

とを更に備えることを特徴とする請求の範囲第17項に記載の情報処理サーバ。

20. 第1端末、第2端末、及び第1端末と第2端末間を仲介する情報処理サーバを含むシステムにおいて、前記情報処理サーバが、

前記第1端末からのアクション要求を、第1レベルの個人情報と共に受信し、

前記第1レベルの個人情報により、前記第1端末を認証し、

前記第1端末に認証情報を発行し、

第1レベルの個人情報よりもセキュリティレベルの高い第2レベルの個人情報を、前記認証情報と共に前記第1端末から受信し、

前記認証情報に基づき、前記アクションに前記第2レベルの個人情報を前記第2端末に送信する。



ことを特徴とする情報処理方法。

21. 前記情報処理サーバは、複数のサーバから構成され、前記第1端末内において、前記複数のサーバの数に対応した複数の情報を、前記複数のサーバに1:1にそれぞれ対応した複数の暗号化鍵でそれぞれ暗号化して、前記複数のサーバの数に対応した複数の暗号化情報を生成して、前記第2レベルの個人情報とし、

前記情報処理サーバが、前記複数のサーバのそれぞれで、前記複数の暗号化情報を順次復号した後、前記第2レベルの個人情報を前記第2端末に送信することを特徴とする請求の範囲第20項に記載の情報処理方法。

22. 前記第1レベルの個人情報は、前記第1端末のメモリ内に格納された固定乱数の組により生成されることを特徴とする請求の範囲第20項に記載の情報処理方法。

23. 前記第1端末は、主第1端末と補助第1端末との組からなり、前記主第1端末に前記認証情報として画像情報を送信し、該画像情報を光学的に読み取った前記補助第1端末の個人情報を、前記第2レベルの個人情報として、前記認証情報と共に前記補助第1端末から受信することを特徴とする請求の範囲第20項に記載の情報処理方法。

1/41

FIG. 1

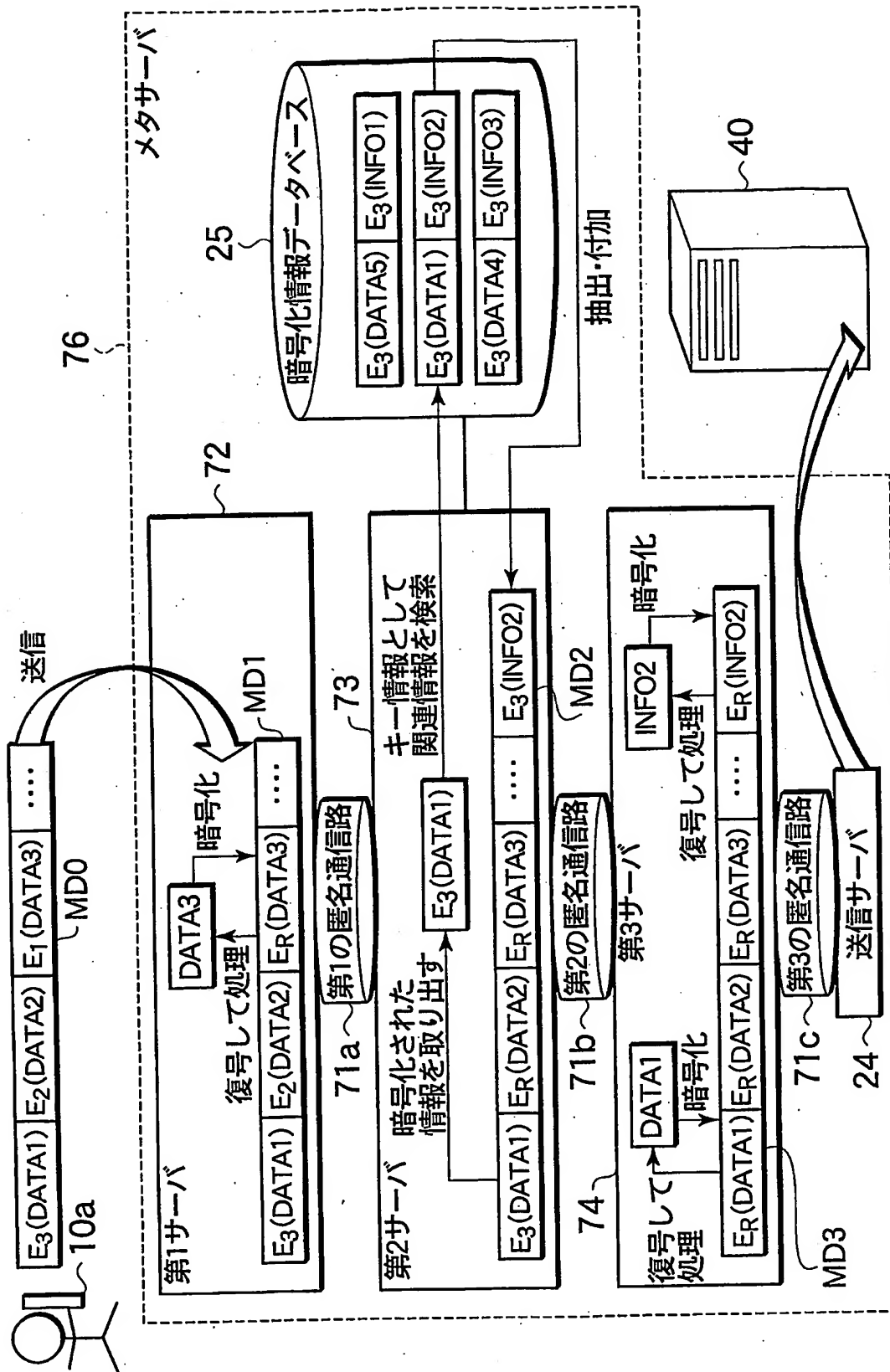


FIG. 2

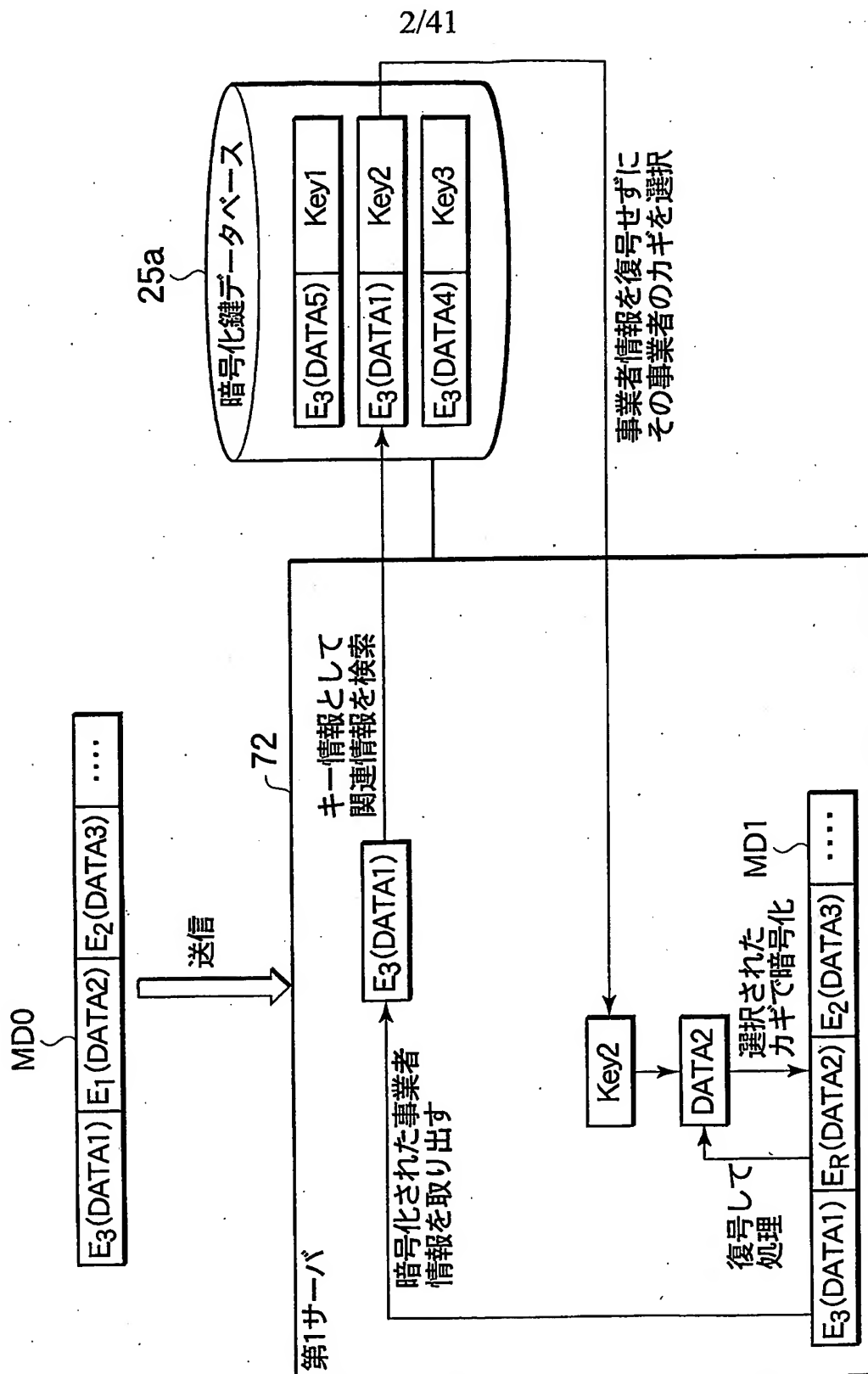
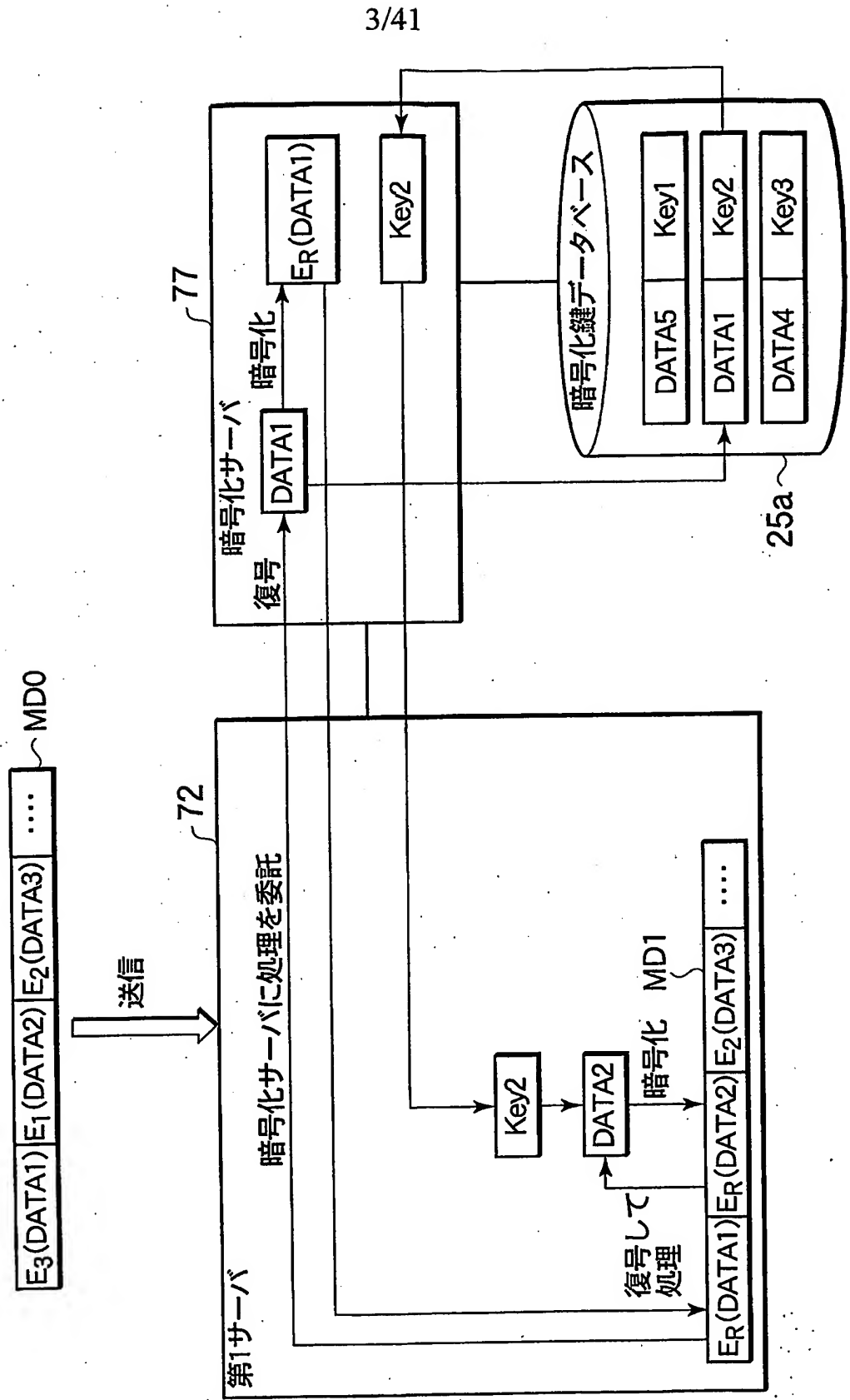


FIG. 3



4/41

FIG. 4

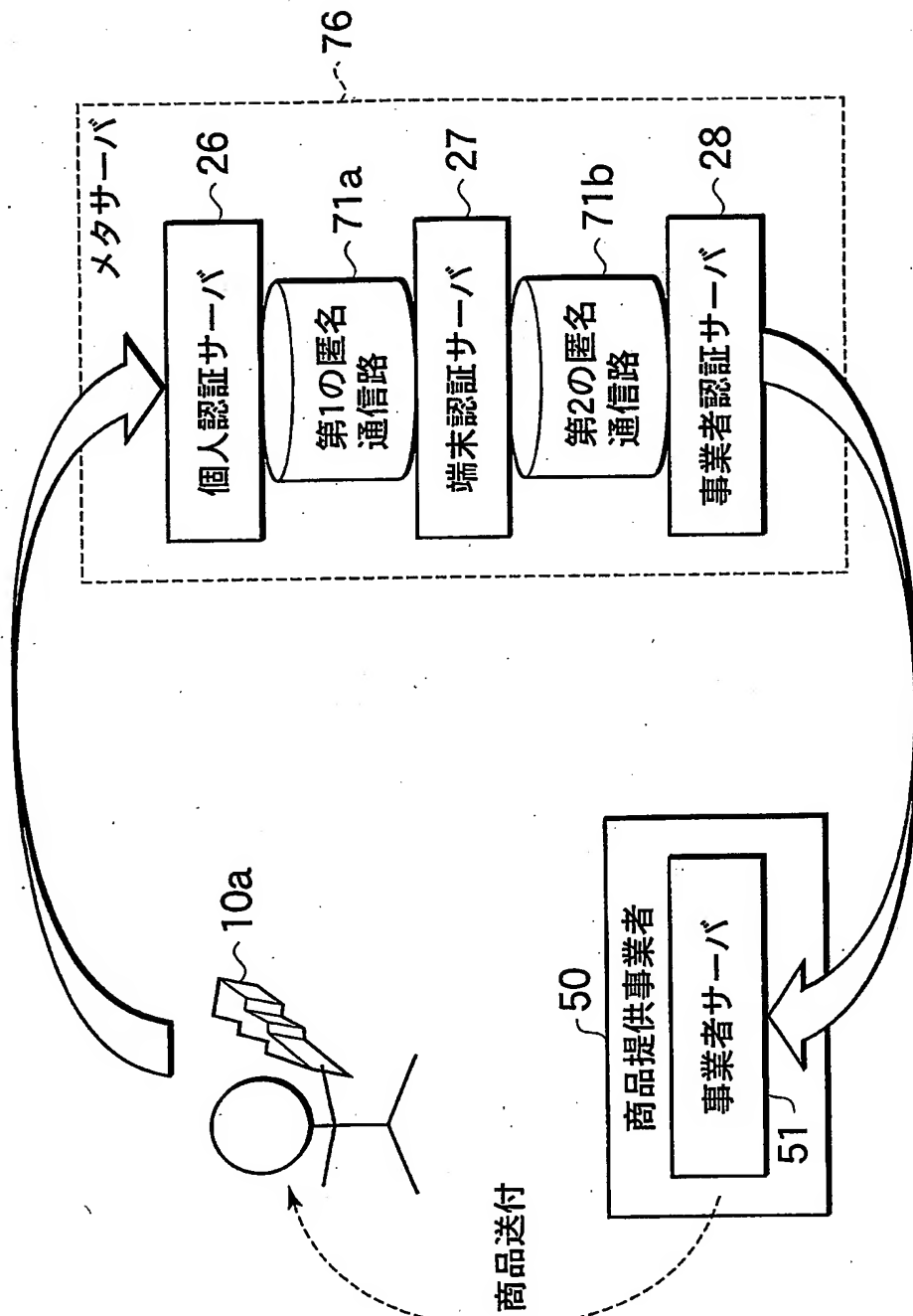


FIG. 5

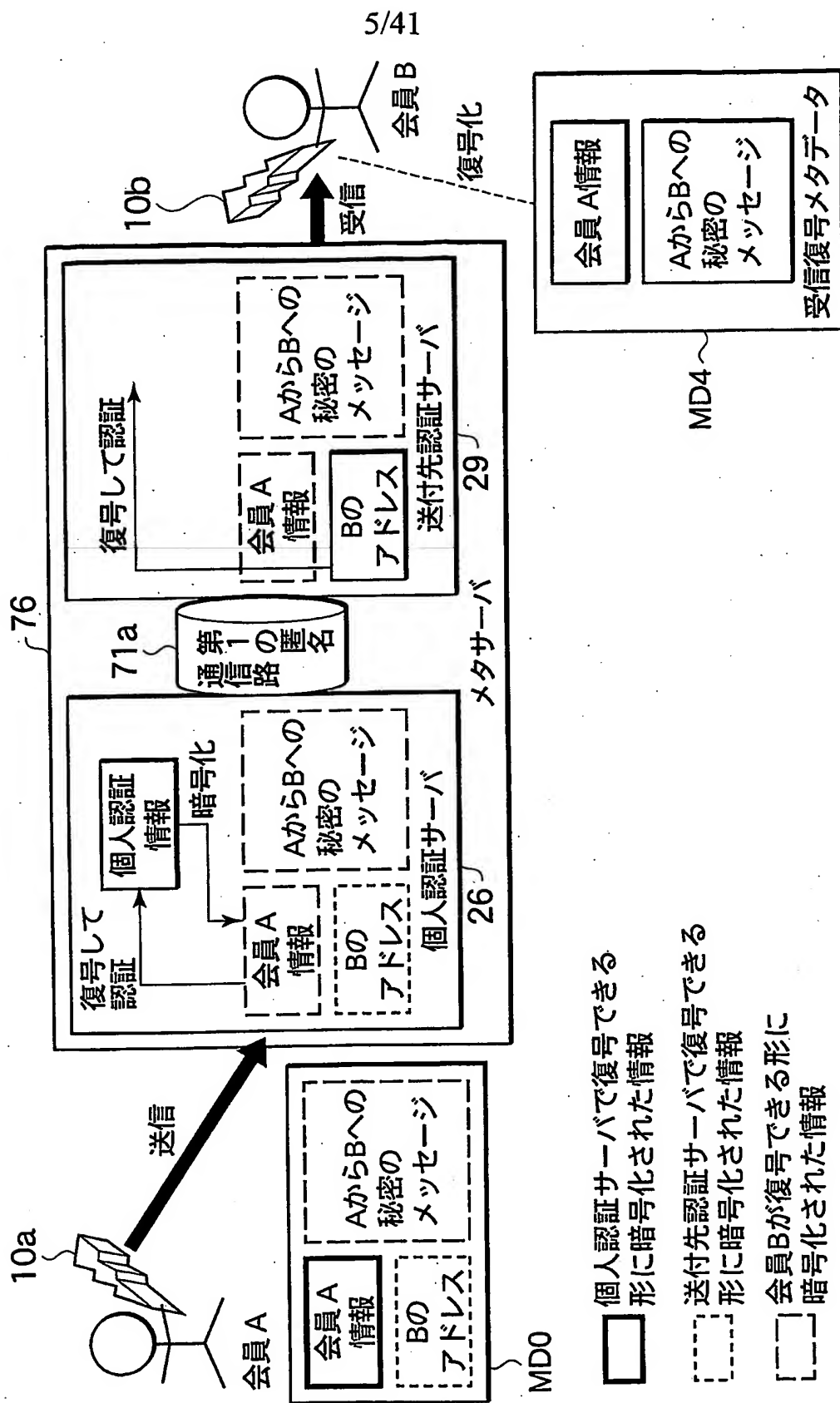


FIG. 6

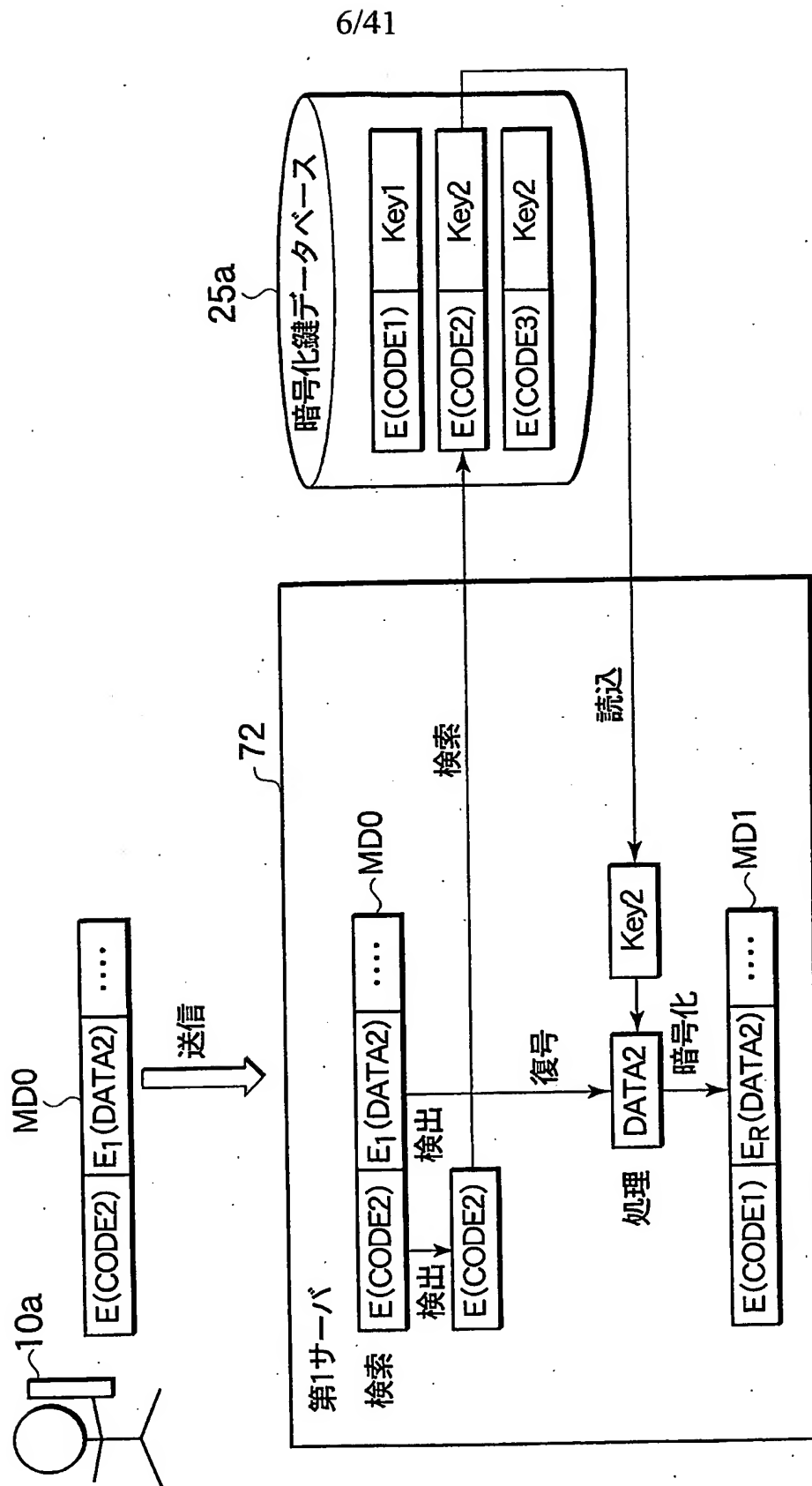


FIG. 7

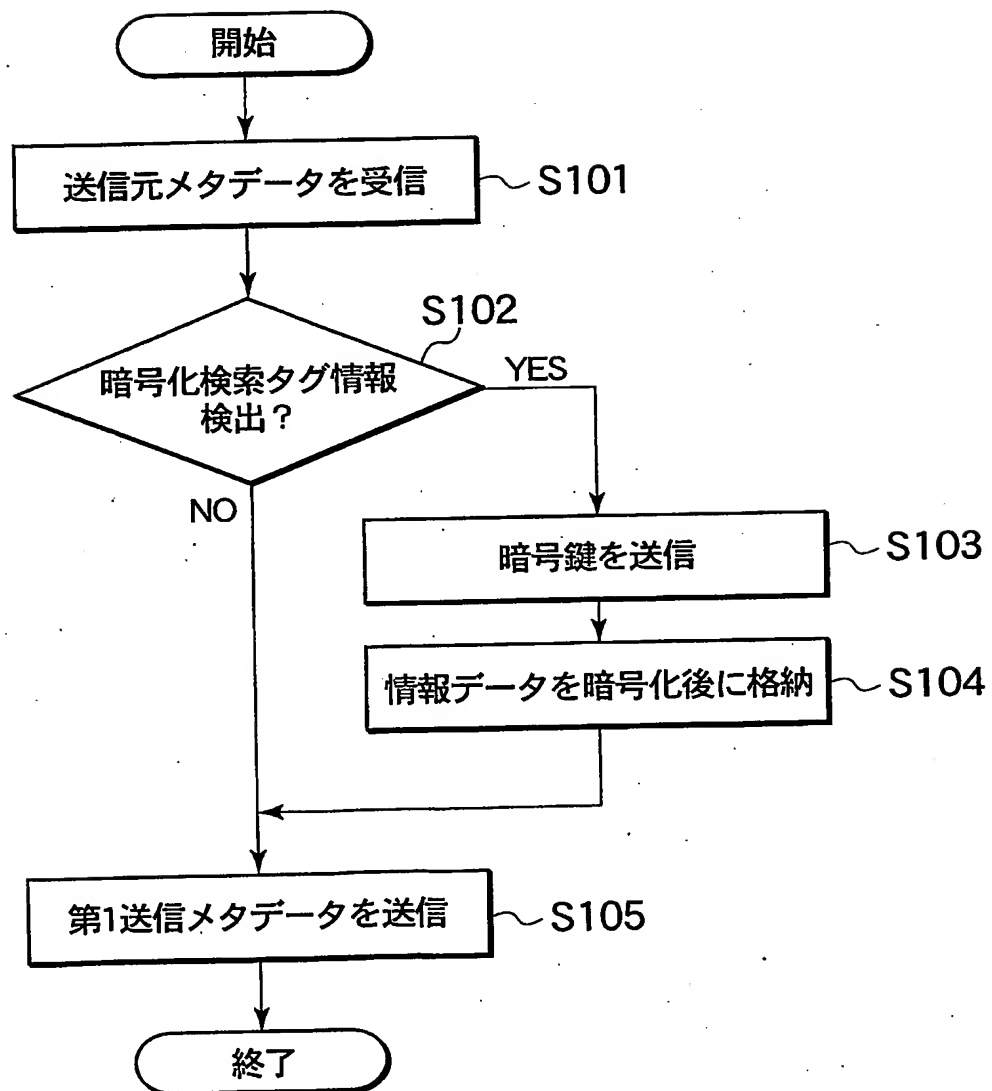
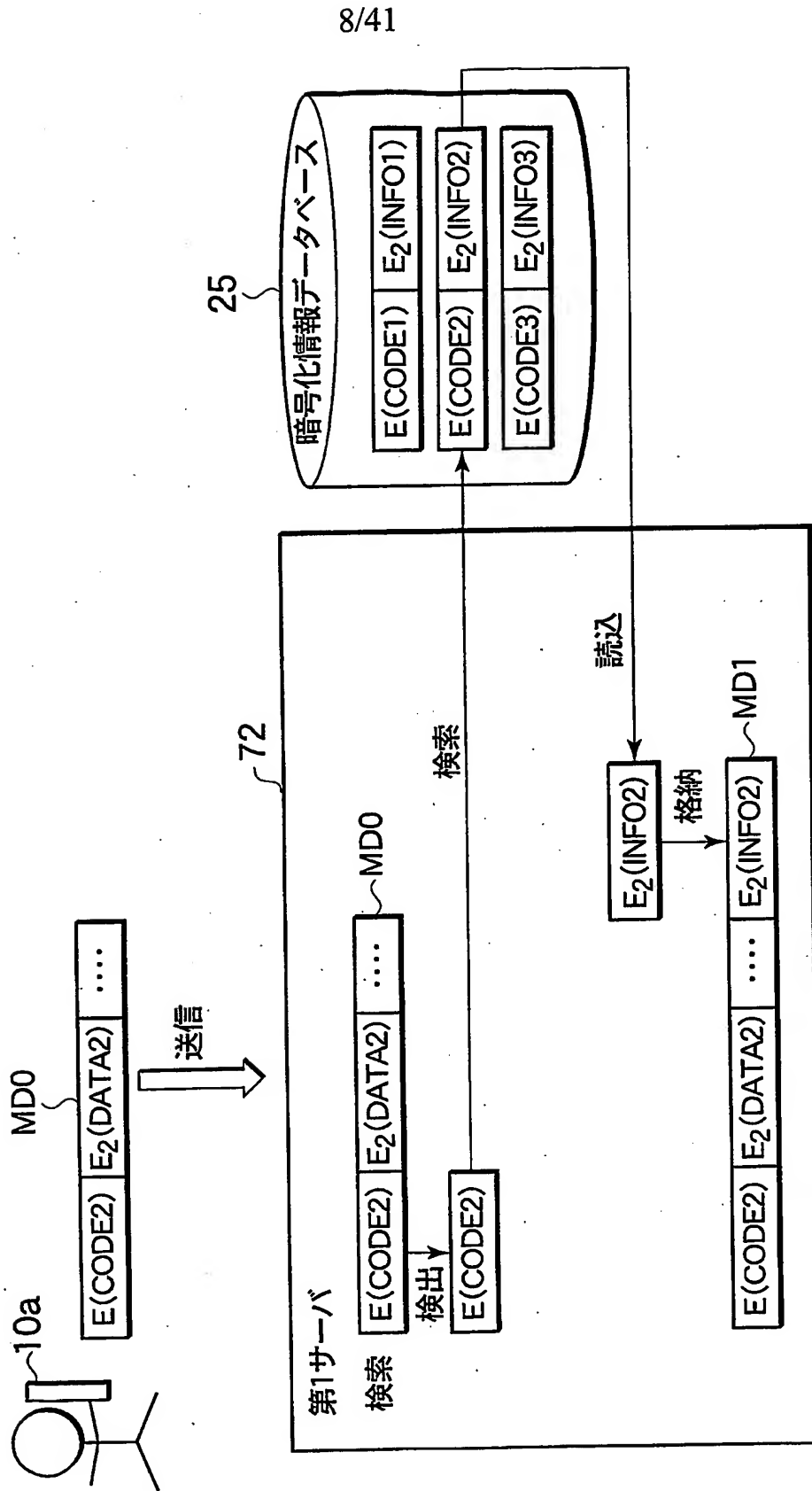




FIG. 8



9/41

FIG. 9

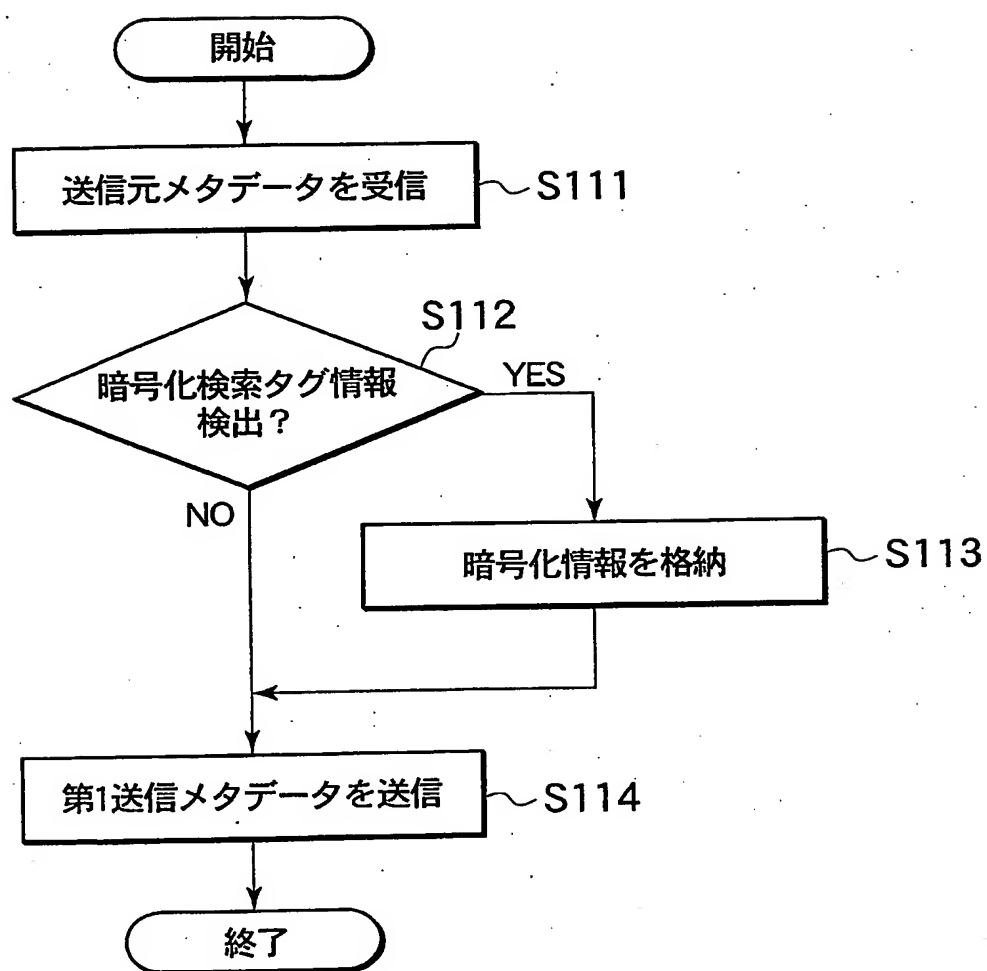
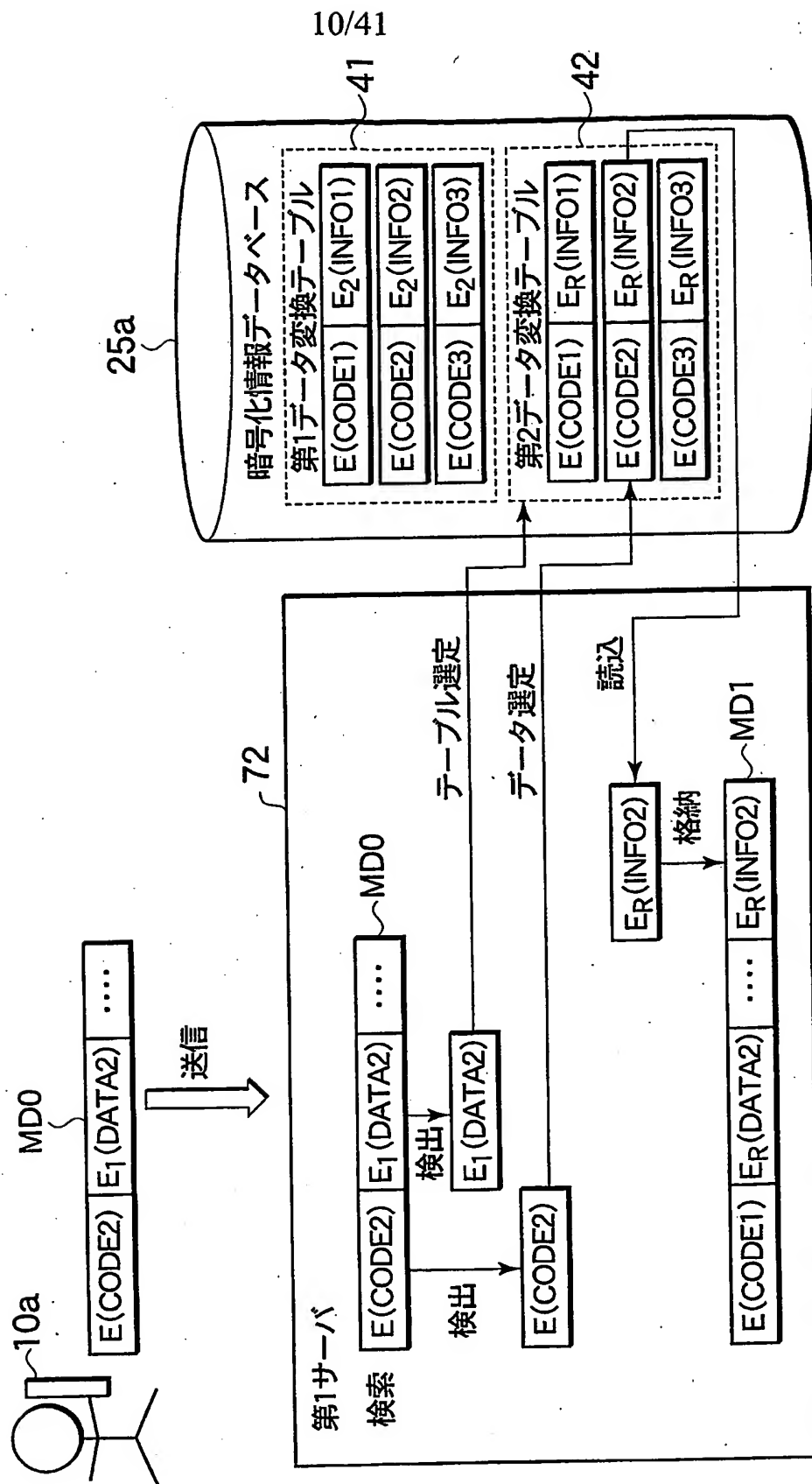
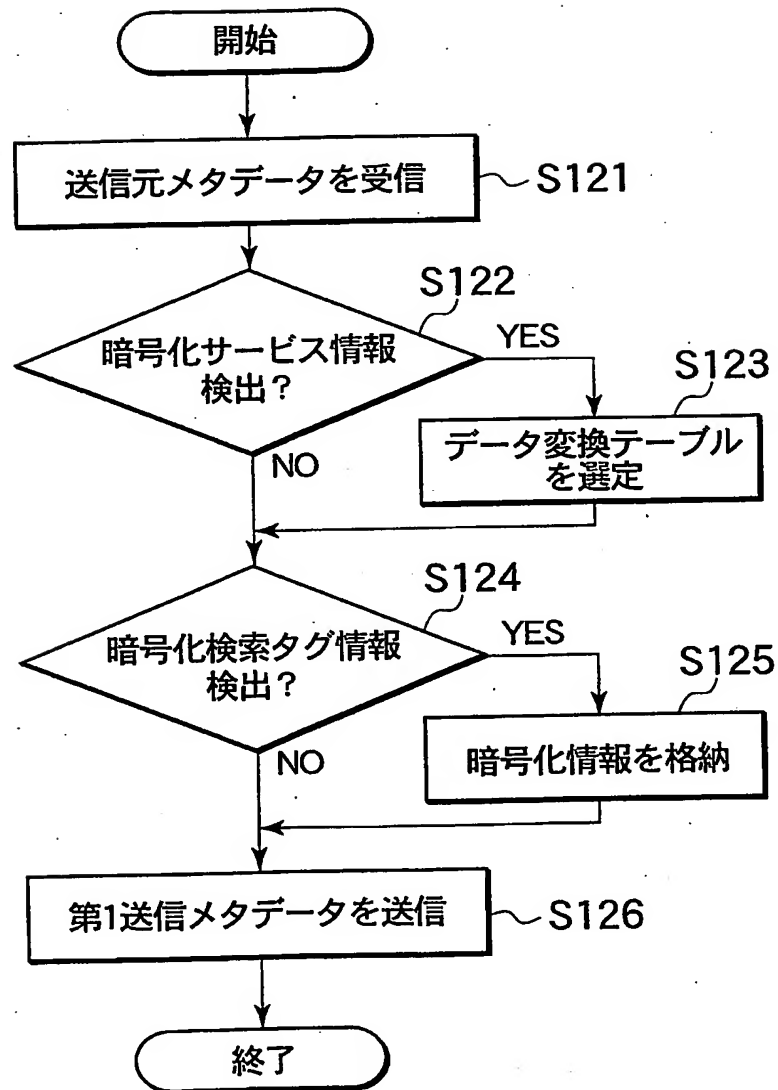


FIG. 10



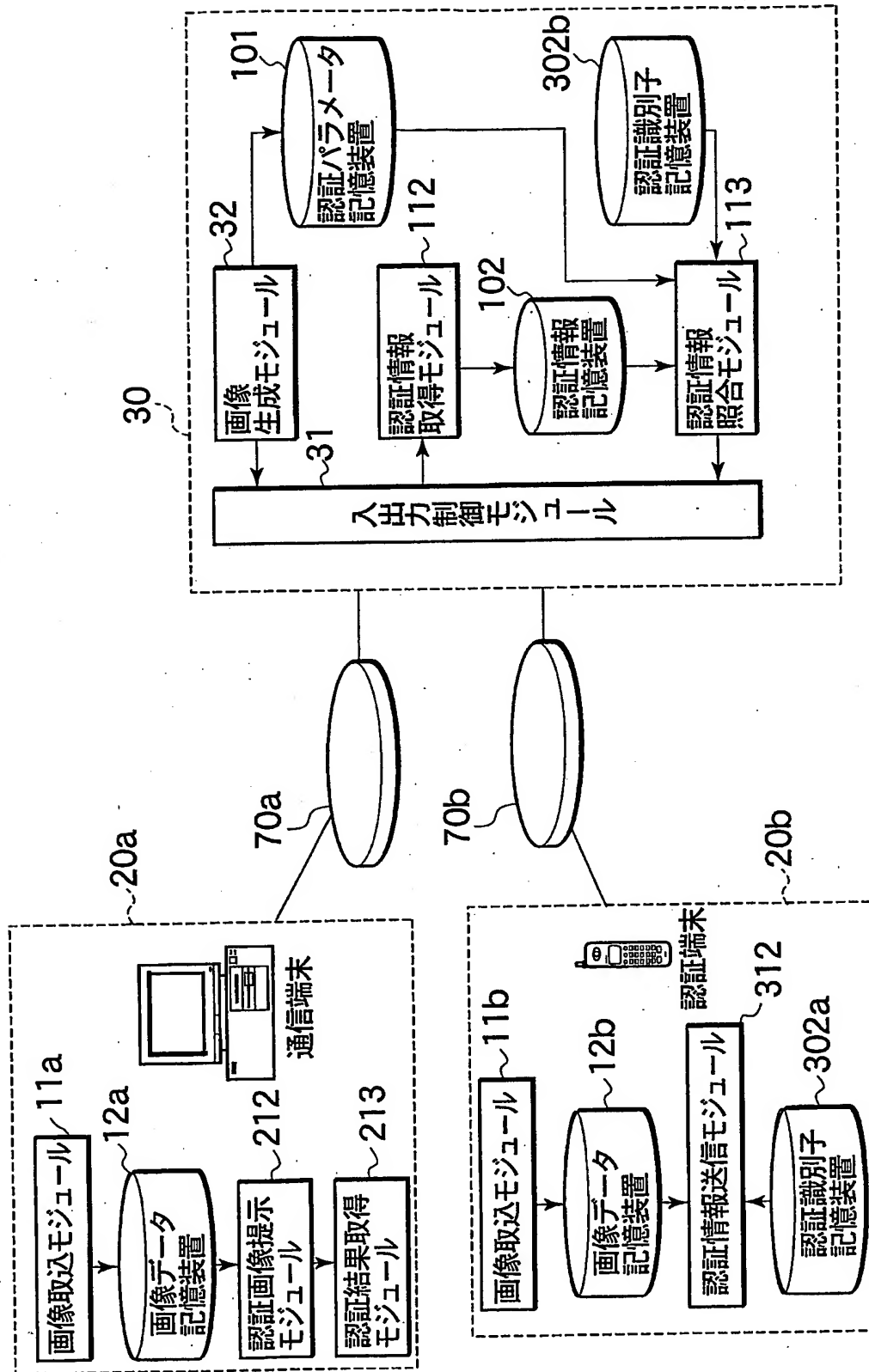
11/41

FIG. 11



12/41

FIG. 12



13/41

FIG. 13

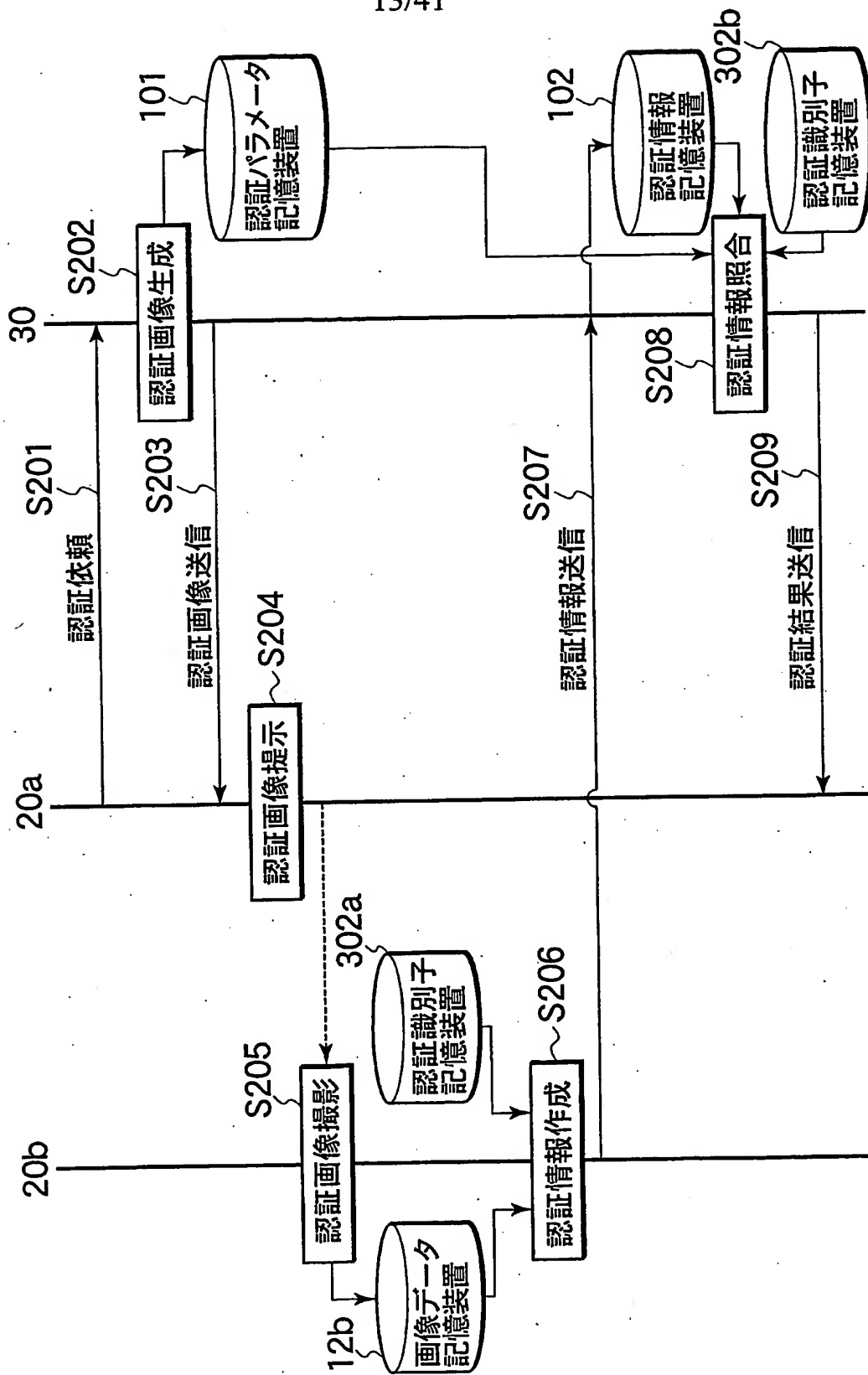
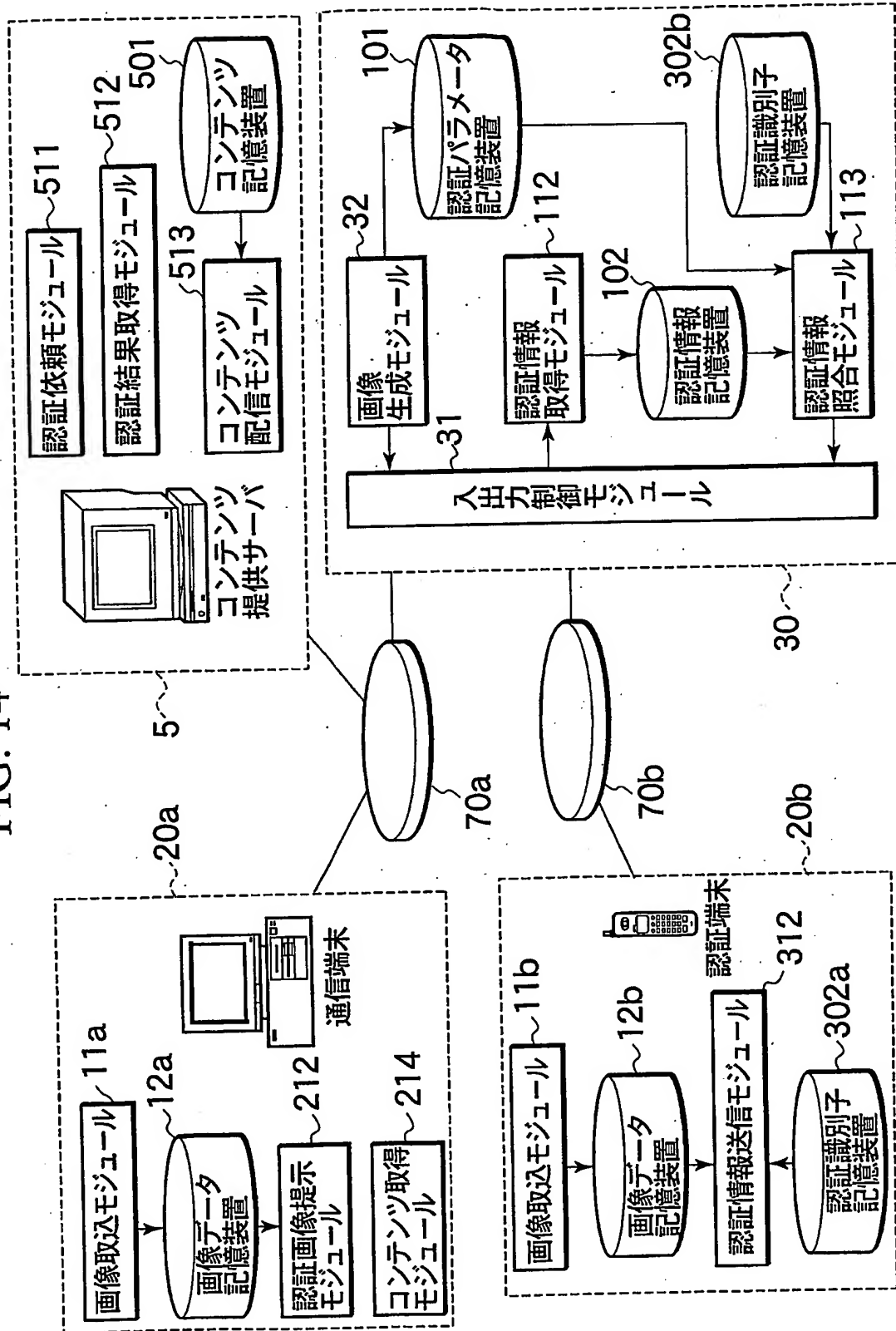
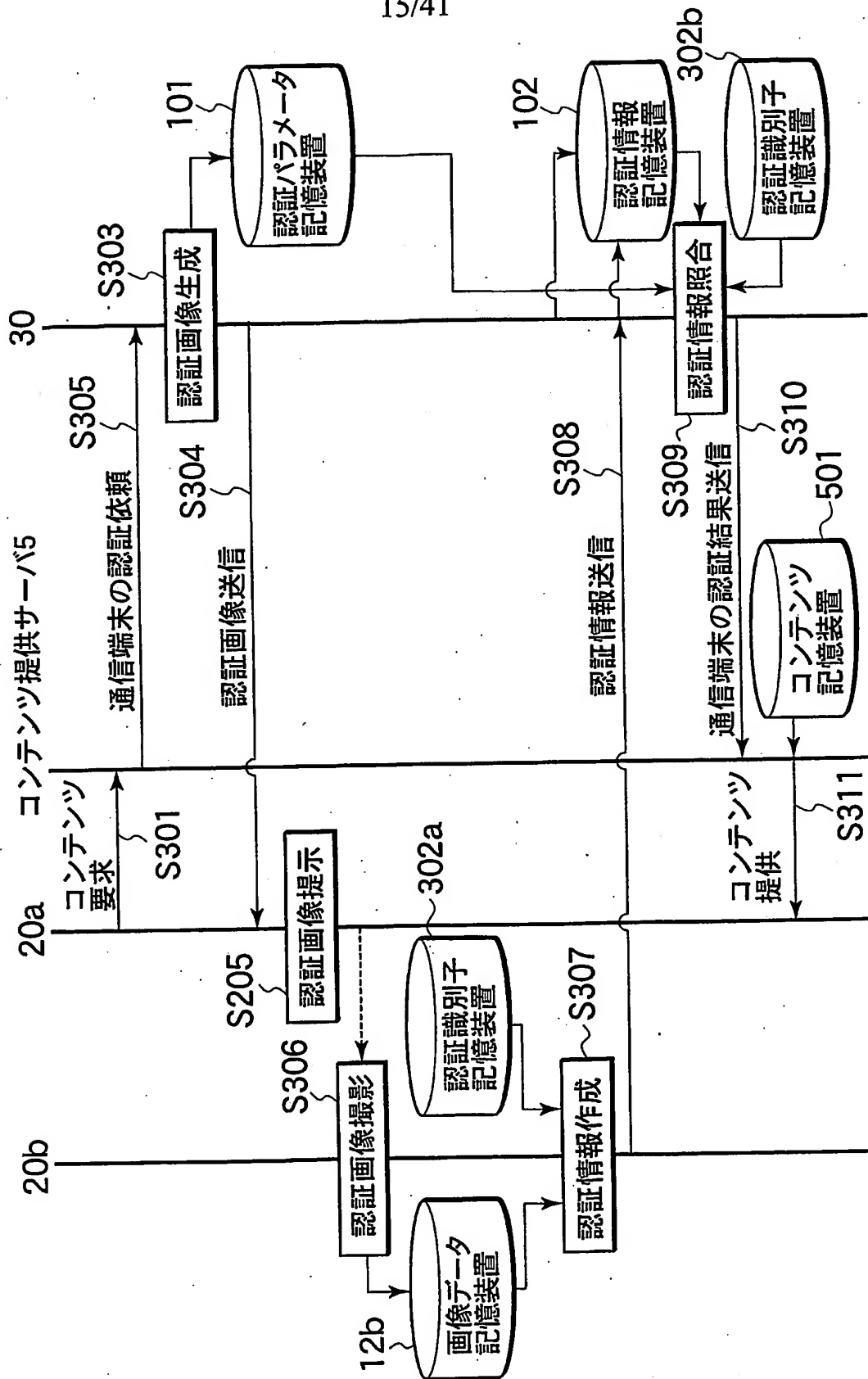


FIG. 14



15/41

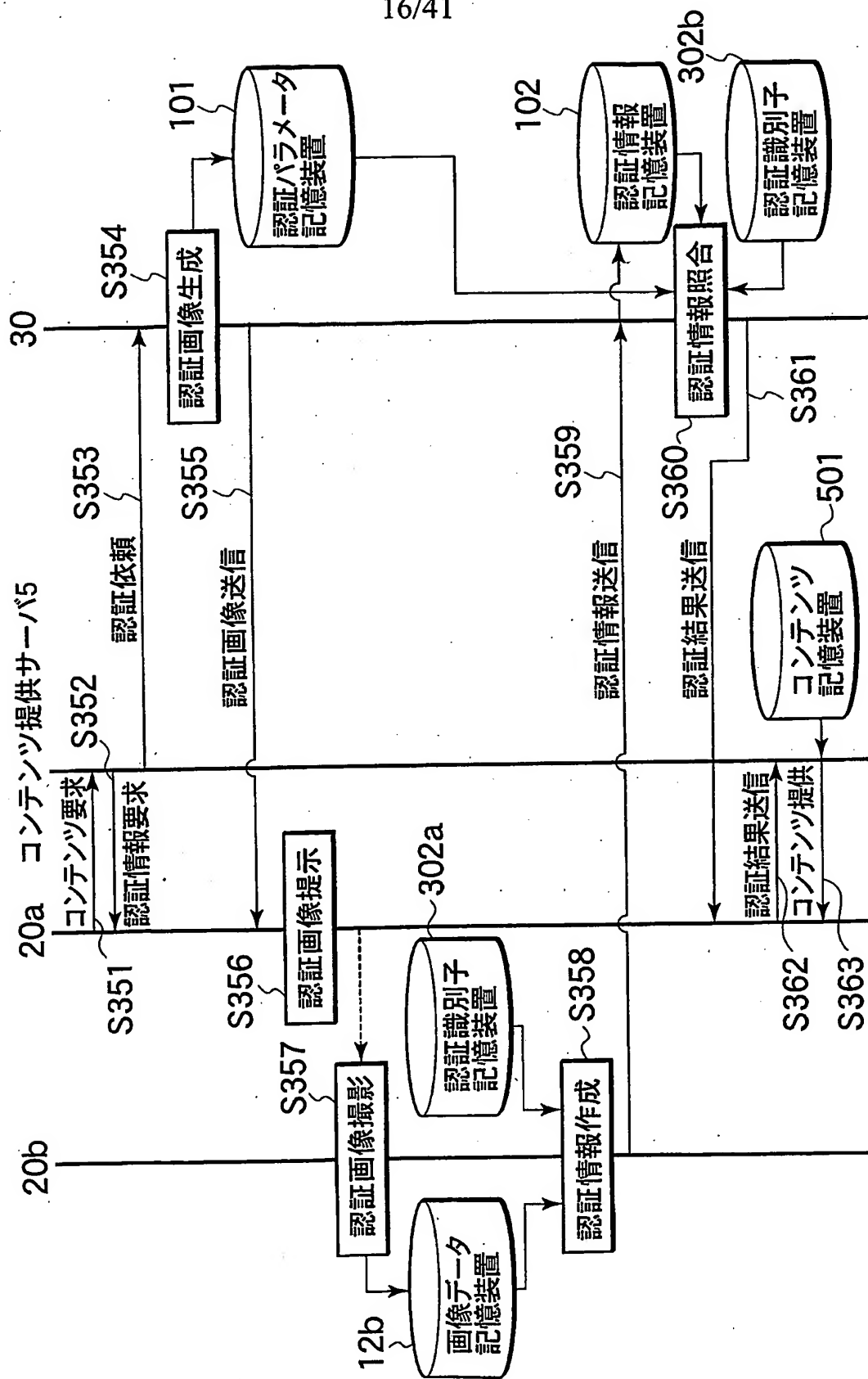
FIG. 15





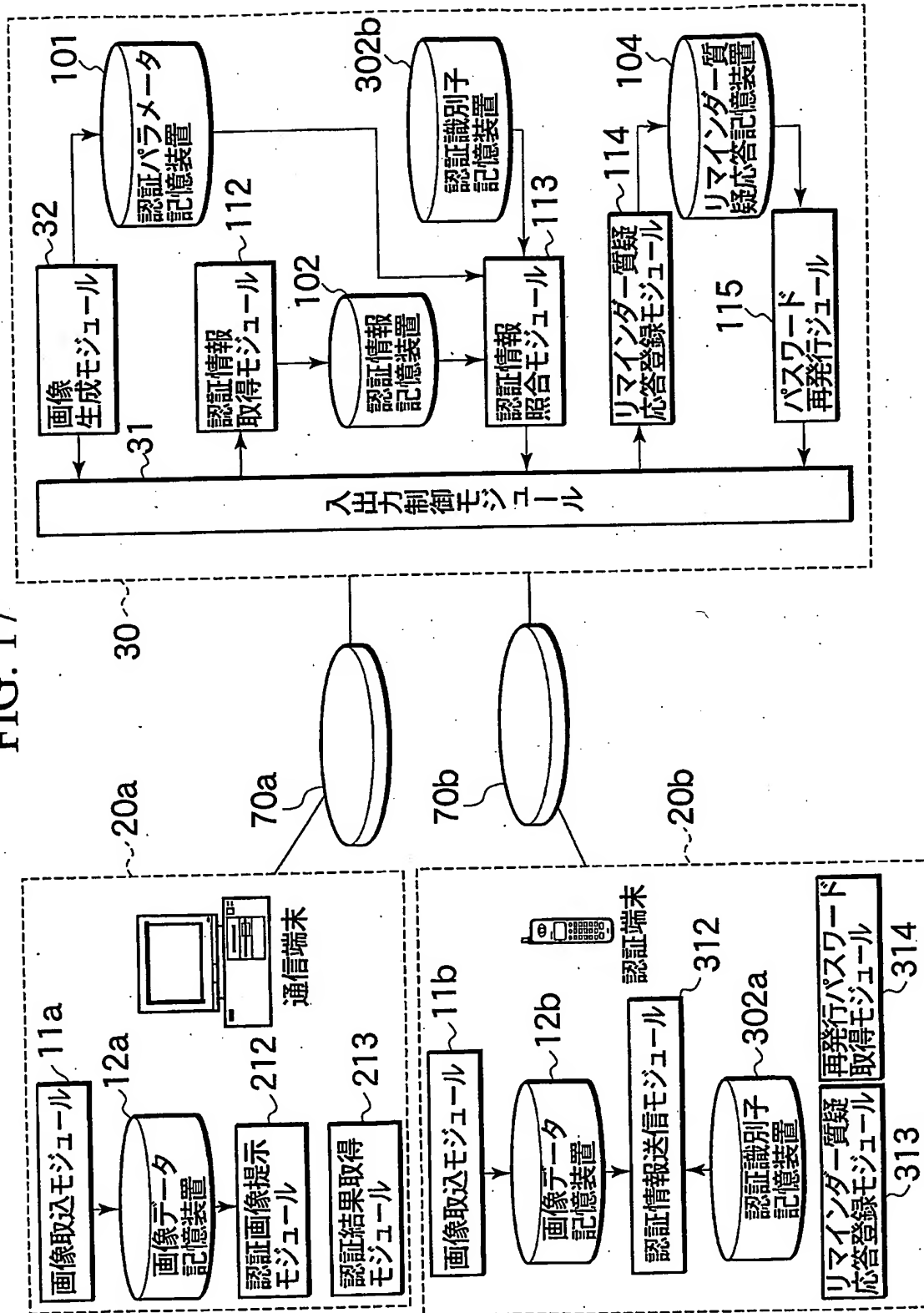
16/41

FIG. 16



17/41

FIG. 17



18/41

FIG. 18

	候補	ジャンル	セレクトリスト	セレクト数
1	お母さんは何日生まれ?	家族	1~31日	31
2	お父さんは何日生まれ?	家族	1~31日	31
3	母親(父親)の旧姓の頭文字は?	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
4	あなたの生まれた市区町村の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
5	初恋の人の苗字の頭文字は?	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
6	最初に飼ったペットの名前の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
7	初めて観た映画のタイトルの頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
8	尊敬する人の苗字の頭文字は?	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
9	母方の祖父の下の名前の頭文字は?	家族	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15
10	いとこは何人いる?	家族	0~14、15以上	16
11	初めての担任の先生の苗字の頭文字	思い出・心	あ・か・が・さ・ざ・た・だ・な・は・ば・ま・や・ら・わ行	15

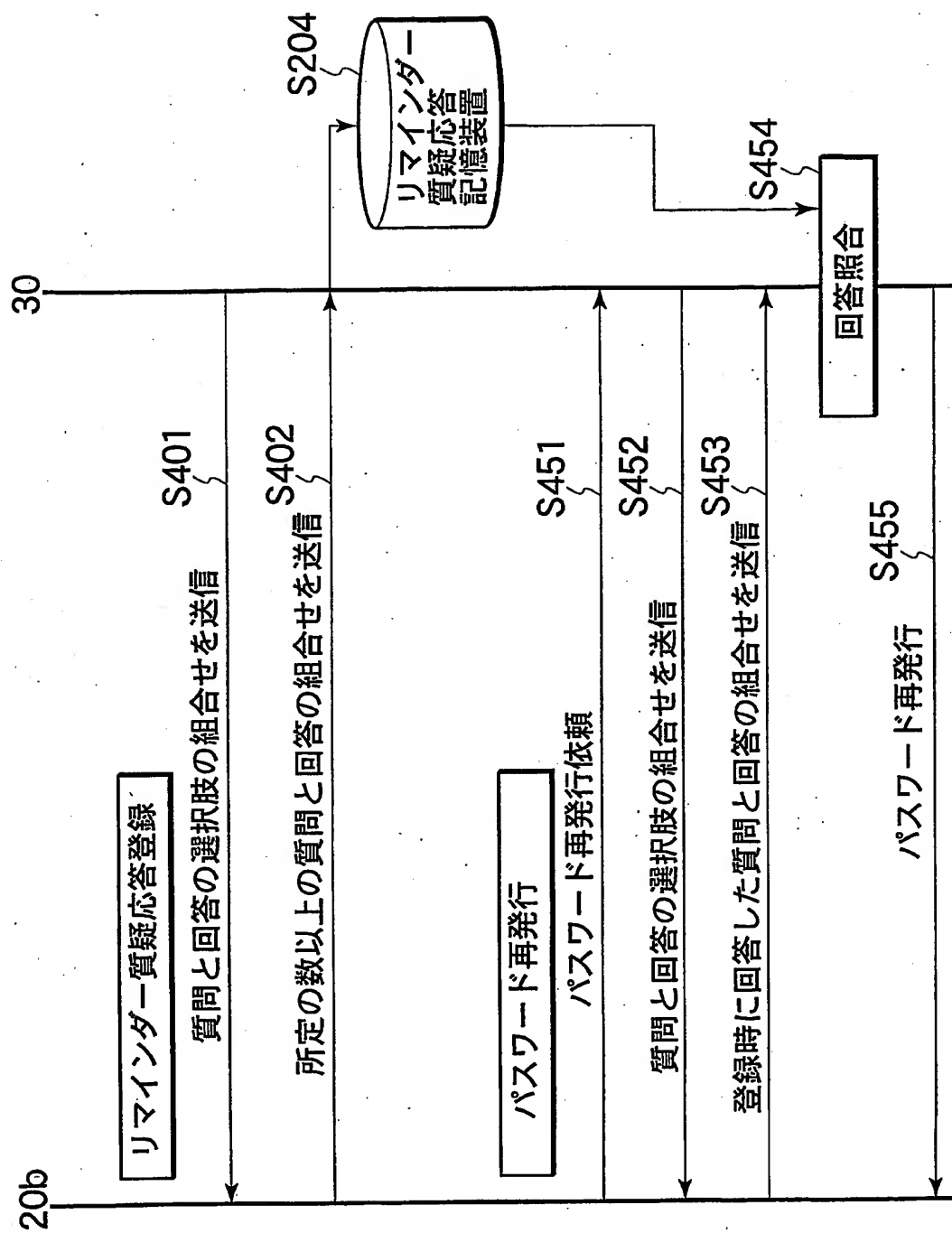
19/41

FIG. 19

英 : A-Z、数 : 0-9	
4桁 (英数)	1,679,616
5桁 (英数)	60,466,176
6桁 (英数)	2,176,782,336
7桁 (英数)	78,364,164,096
8桁 (英数)	2,821,109,907,456
4桁 (数)	10,000
5桁 (数)	100,000
6桁 (数)	1,000,000
7桁 (数)	10,000,000
8桁 (数)	100,000,000

20/41

FIG. 20



21/41

FIG. 21

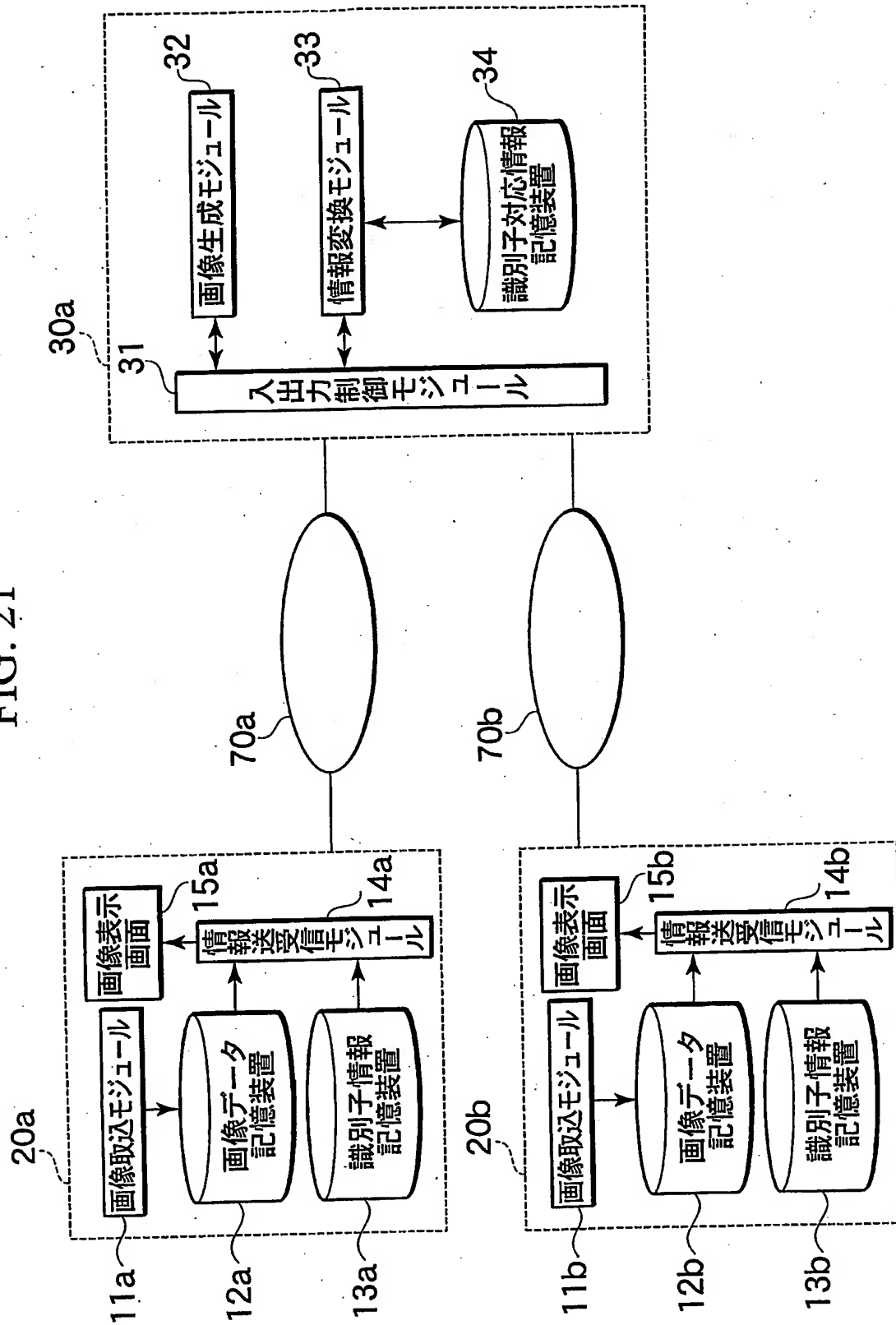
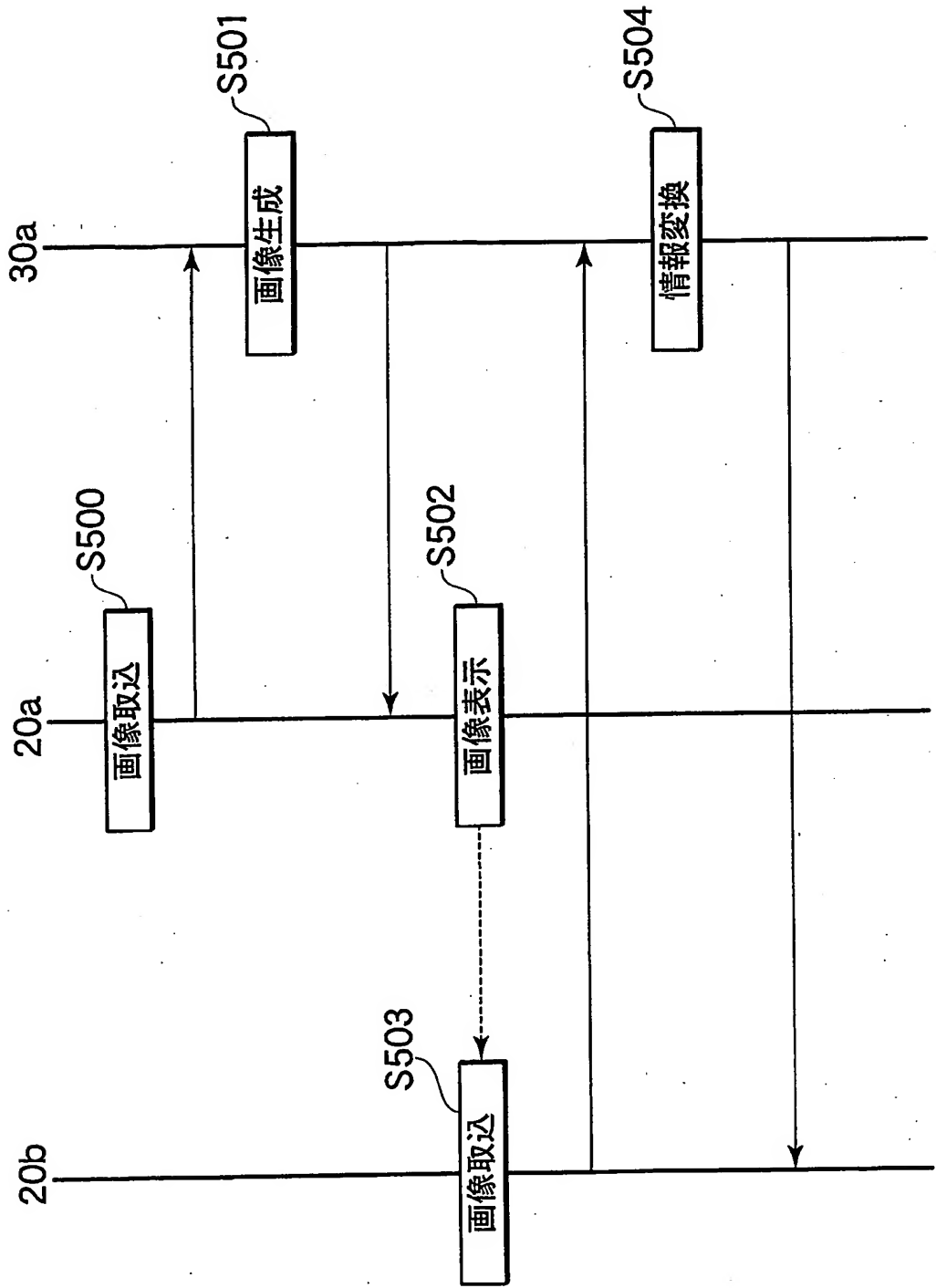
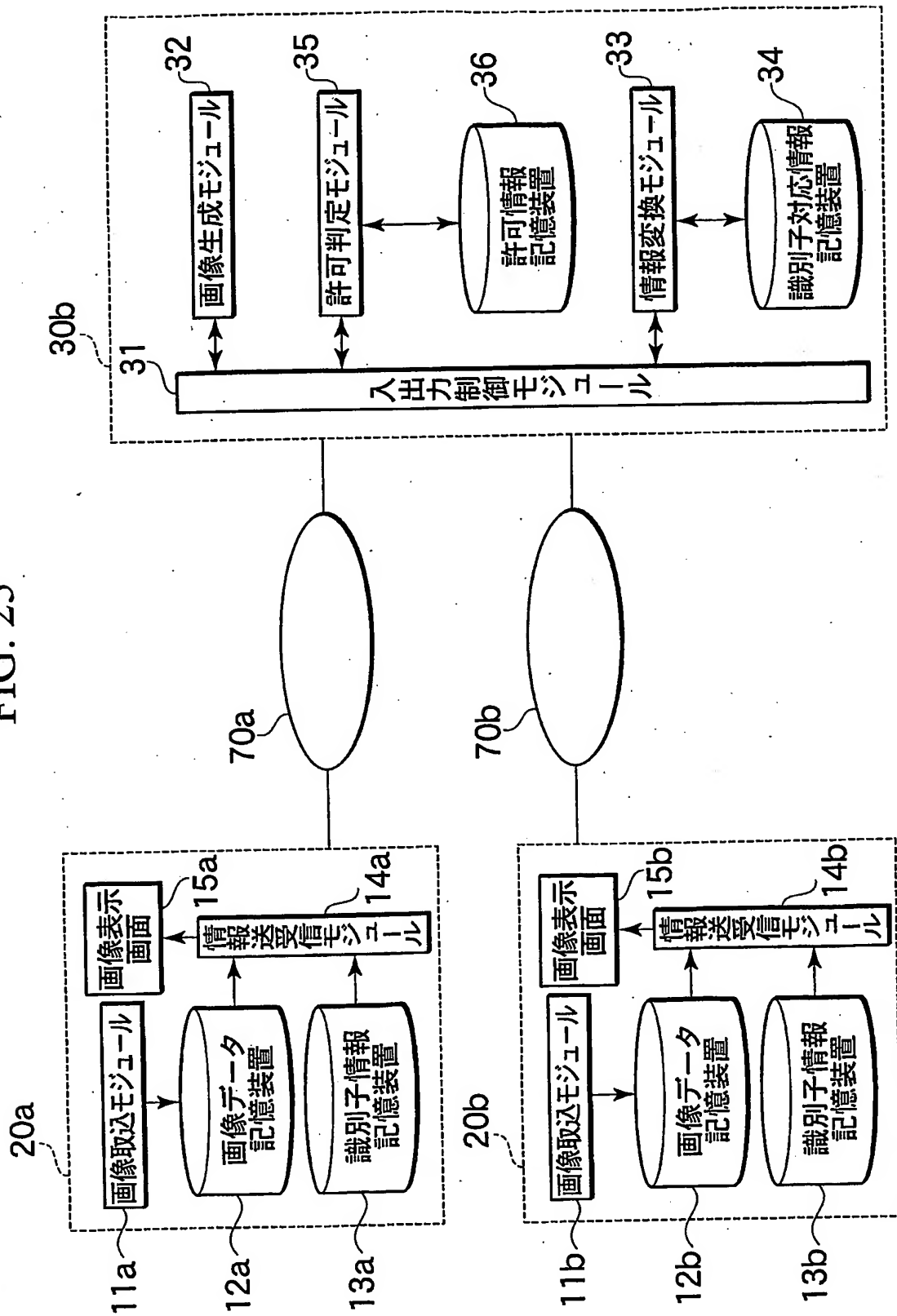


FIG. 22



23/41

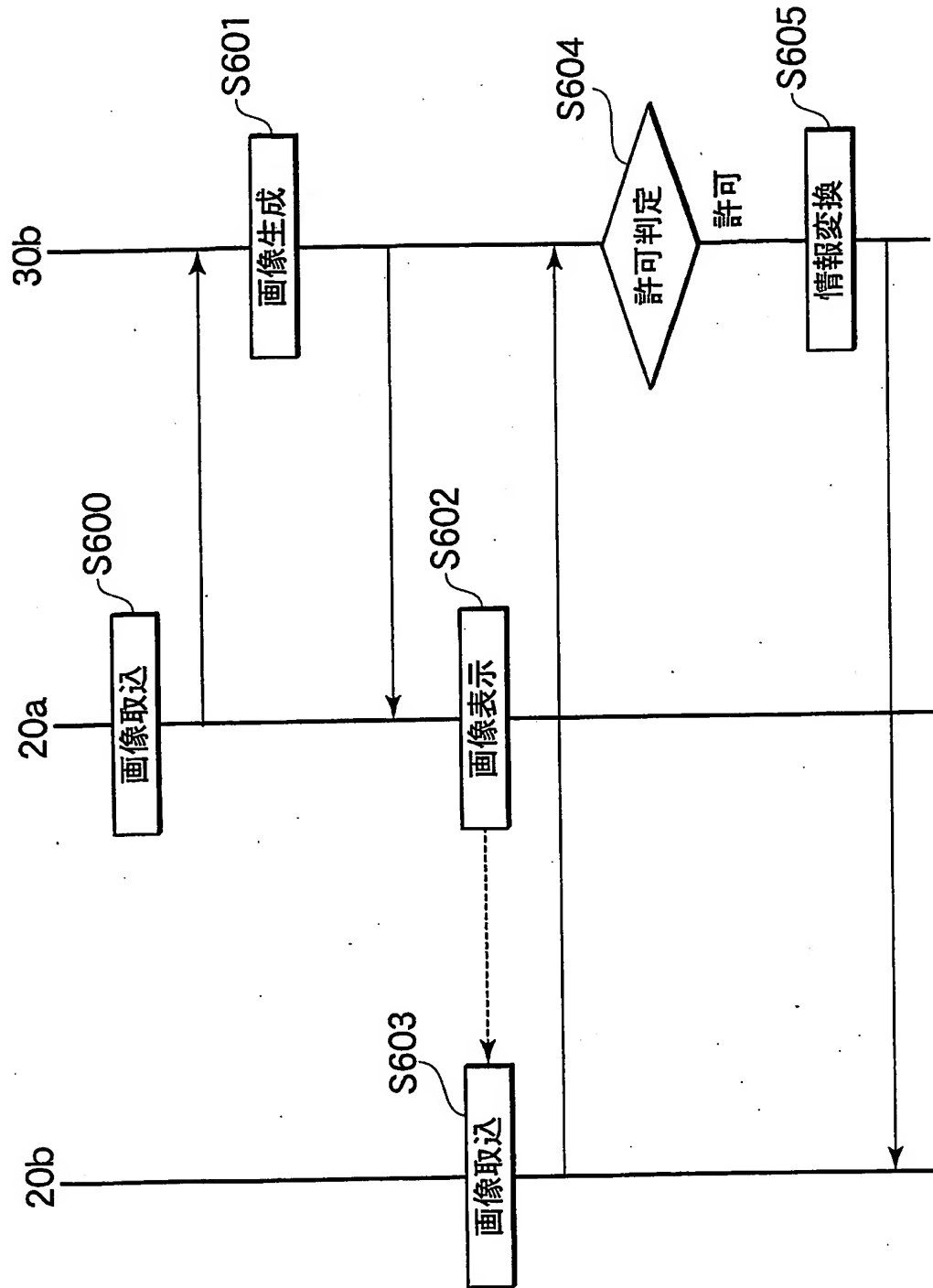
FIG. 23





24/41

FIG. 24



25/41

FIG. 25

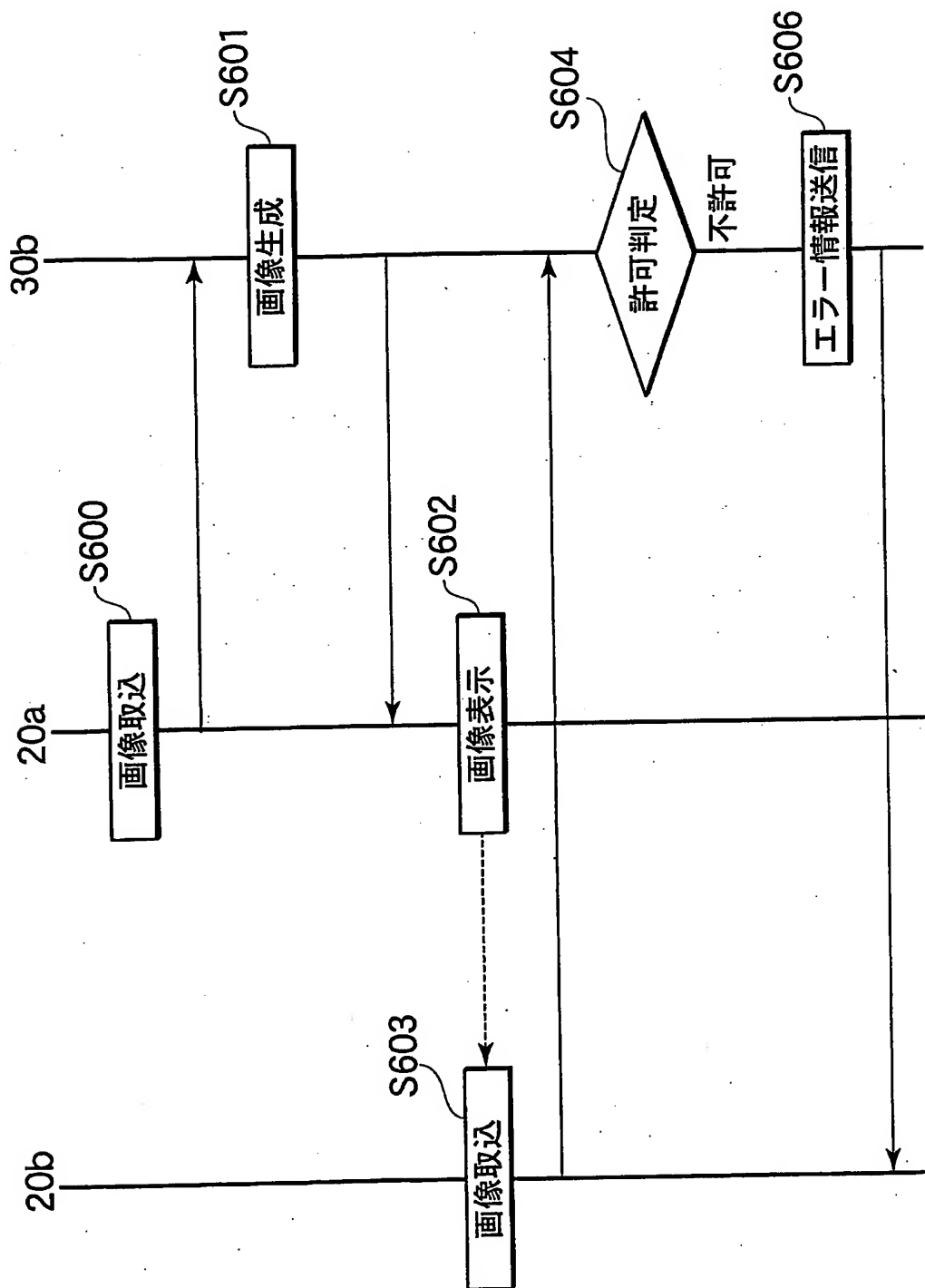
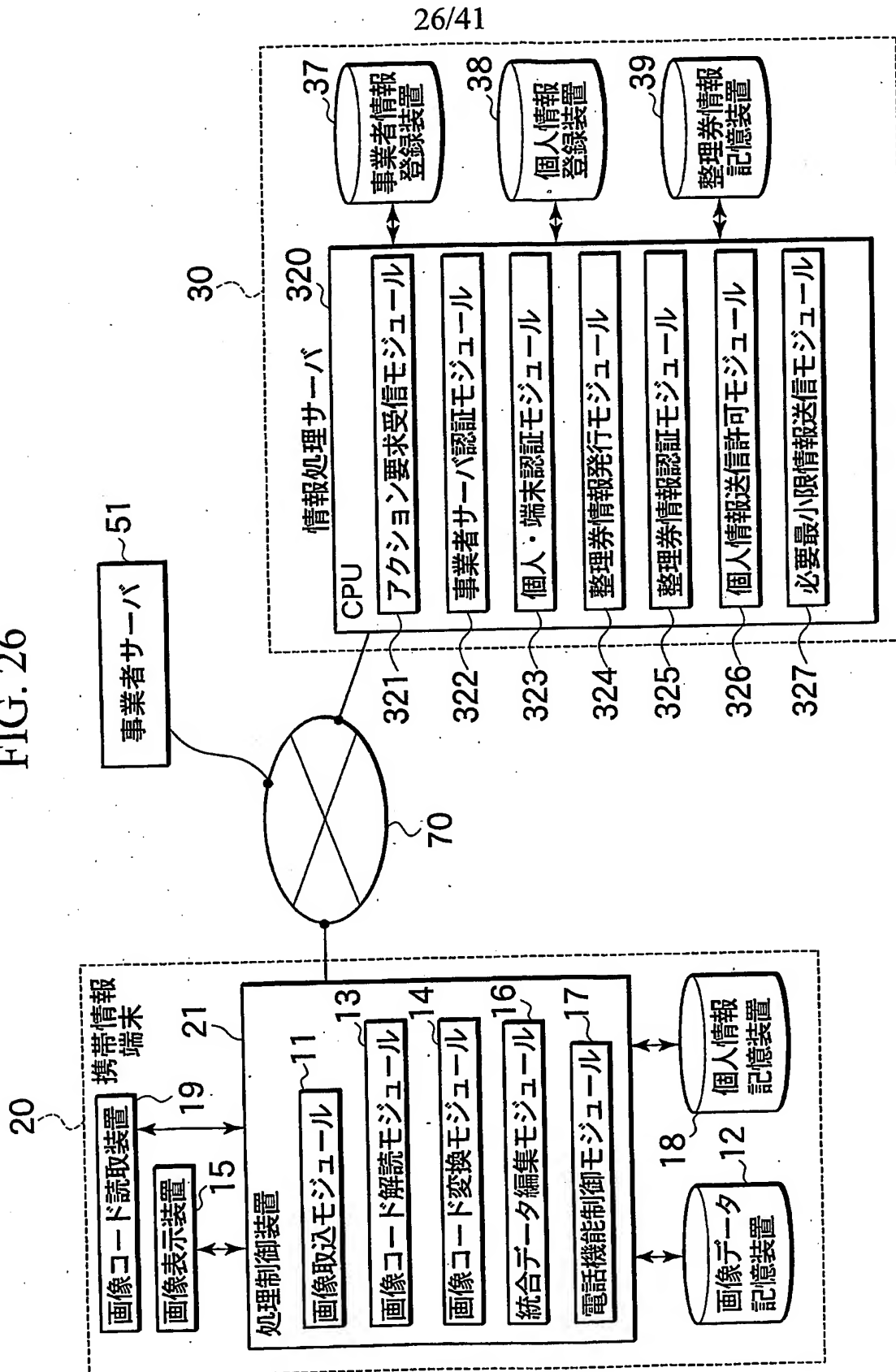
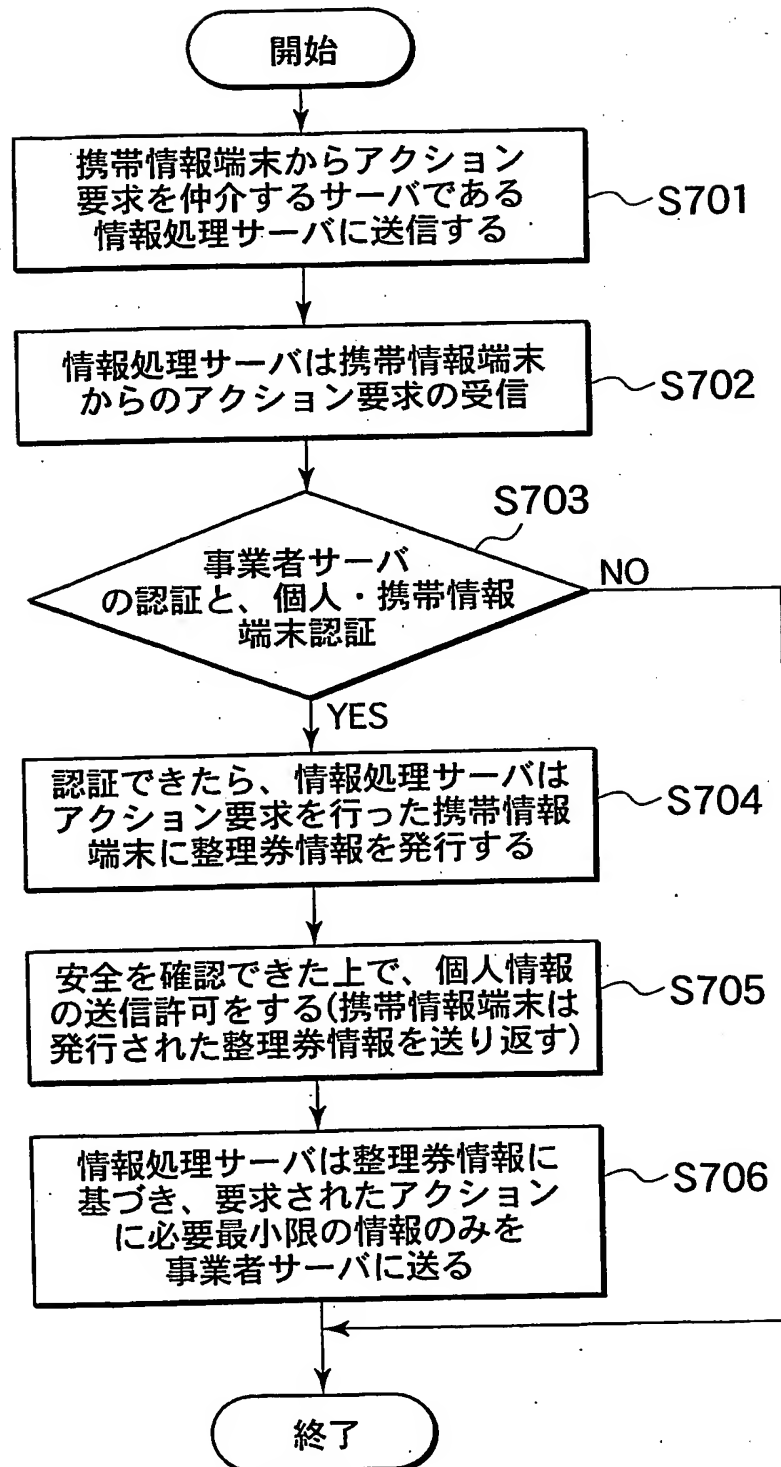


FIG. 26



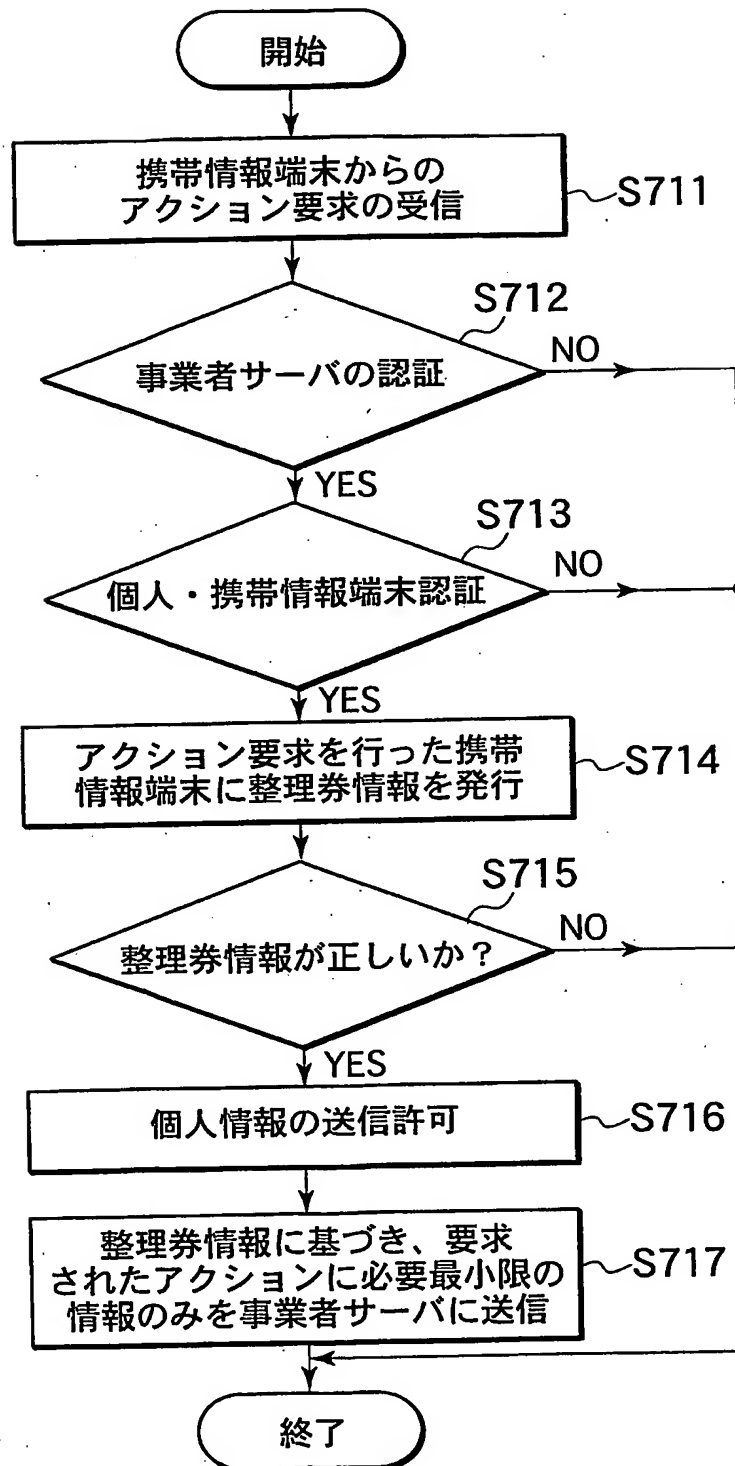
27/41

FIG. 27



28/41

FIG. 28



29/41

FIG. 29

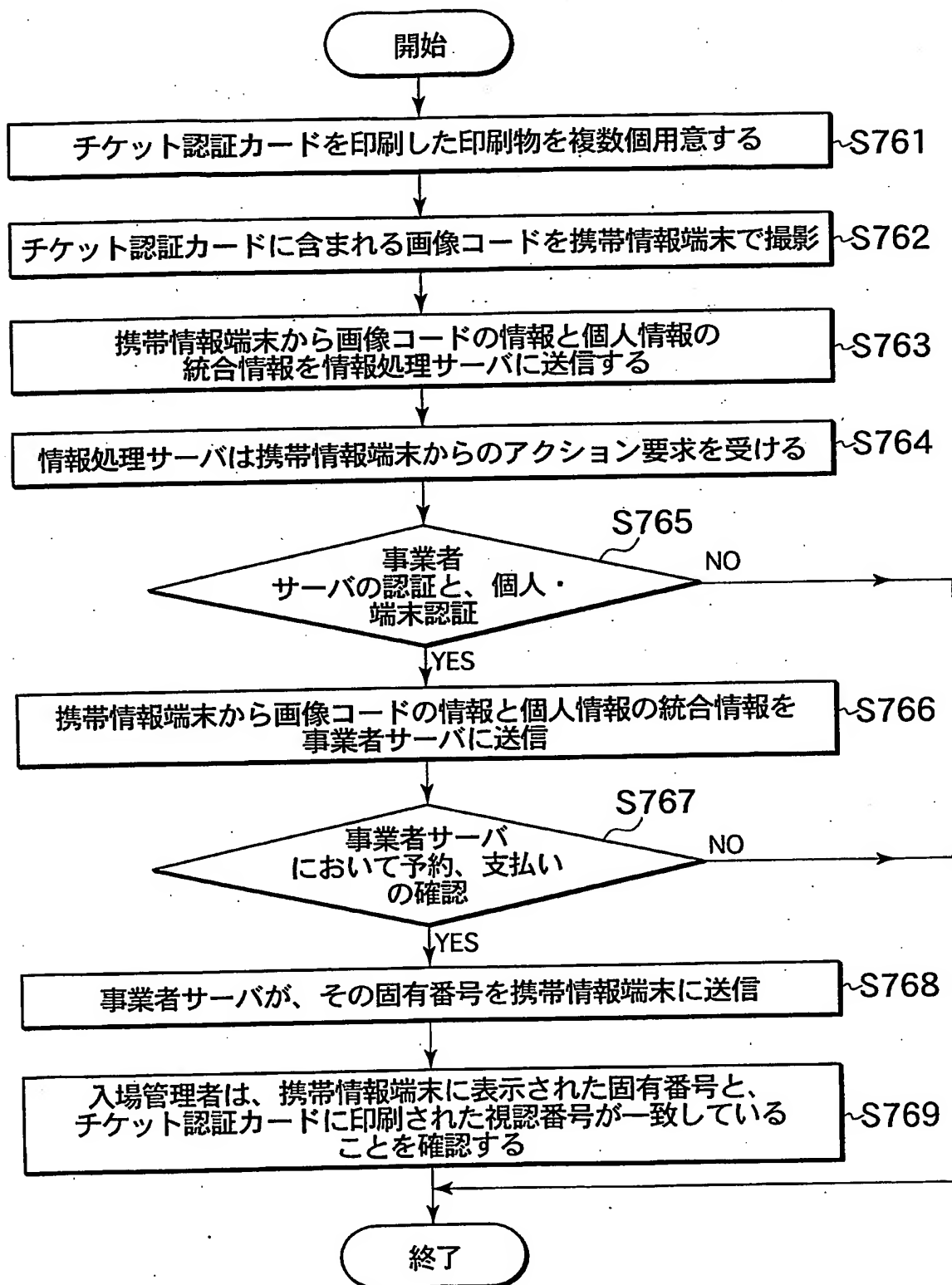


FIG.30

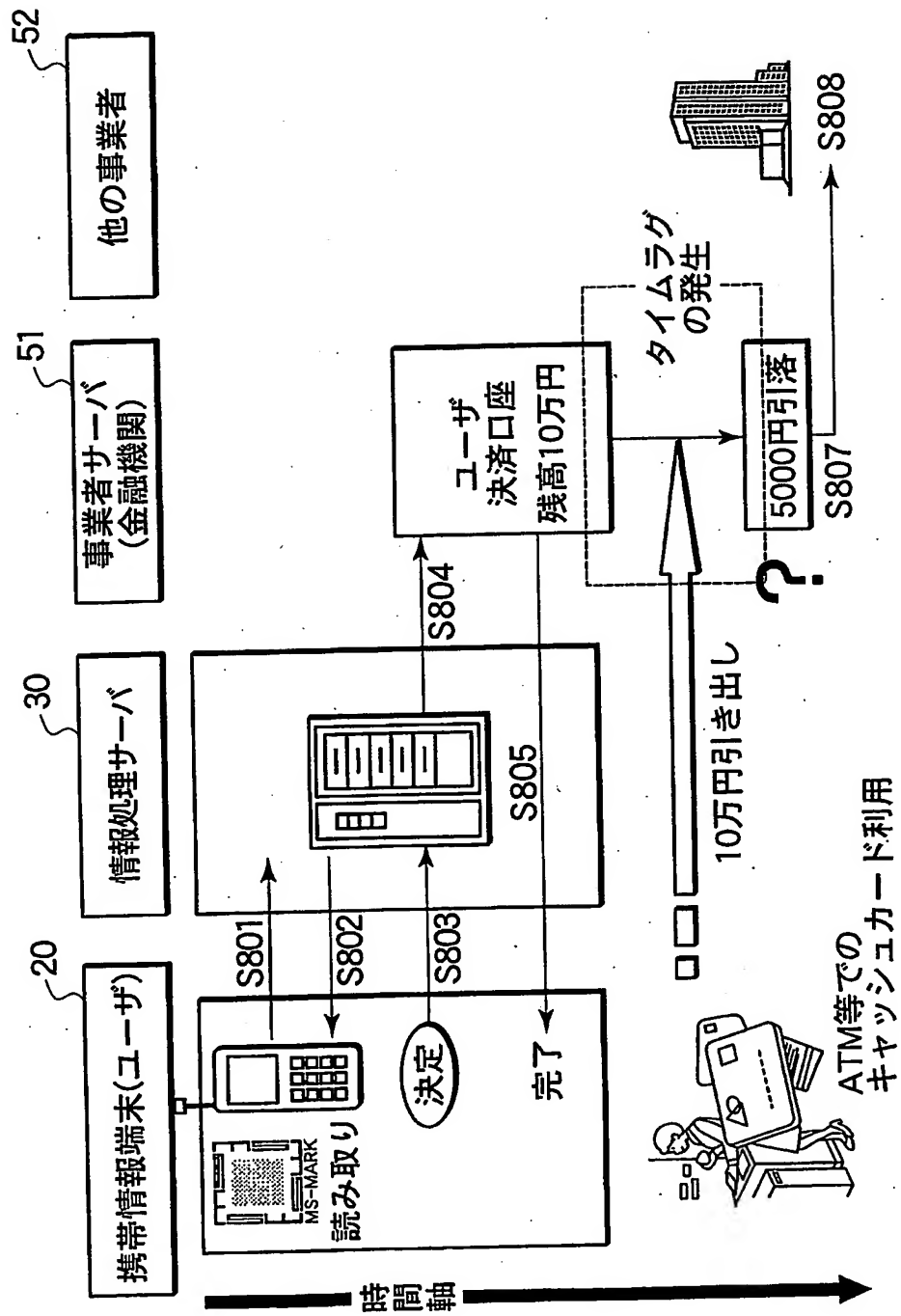


FIG. 31

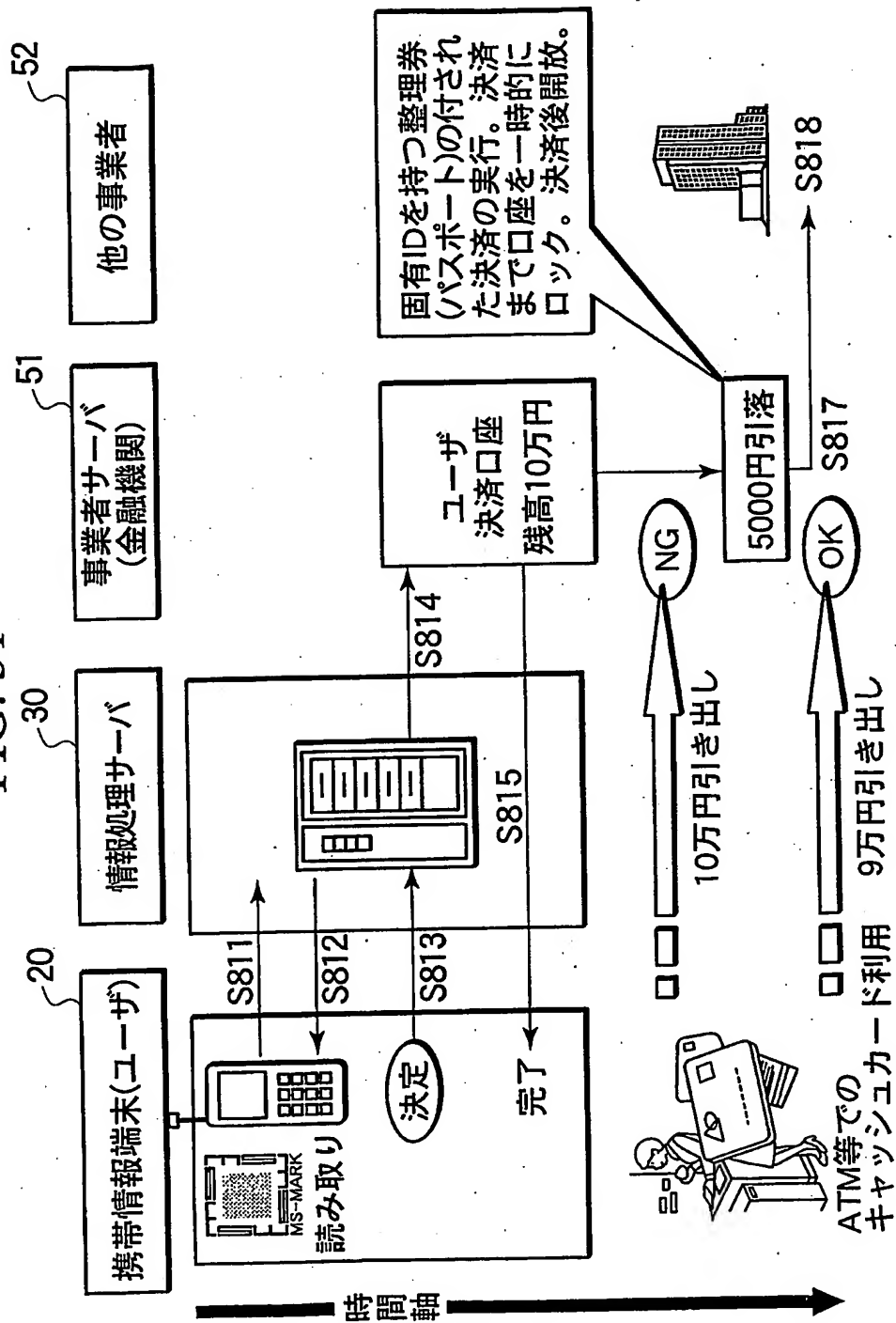
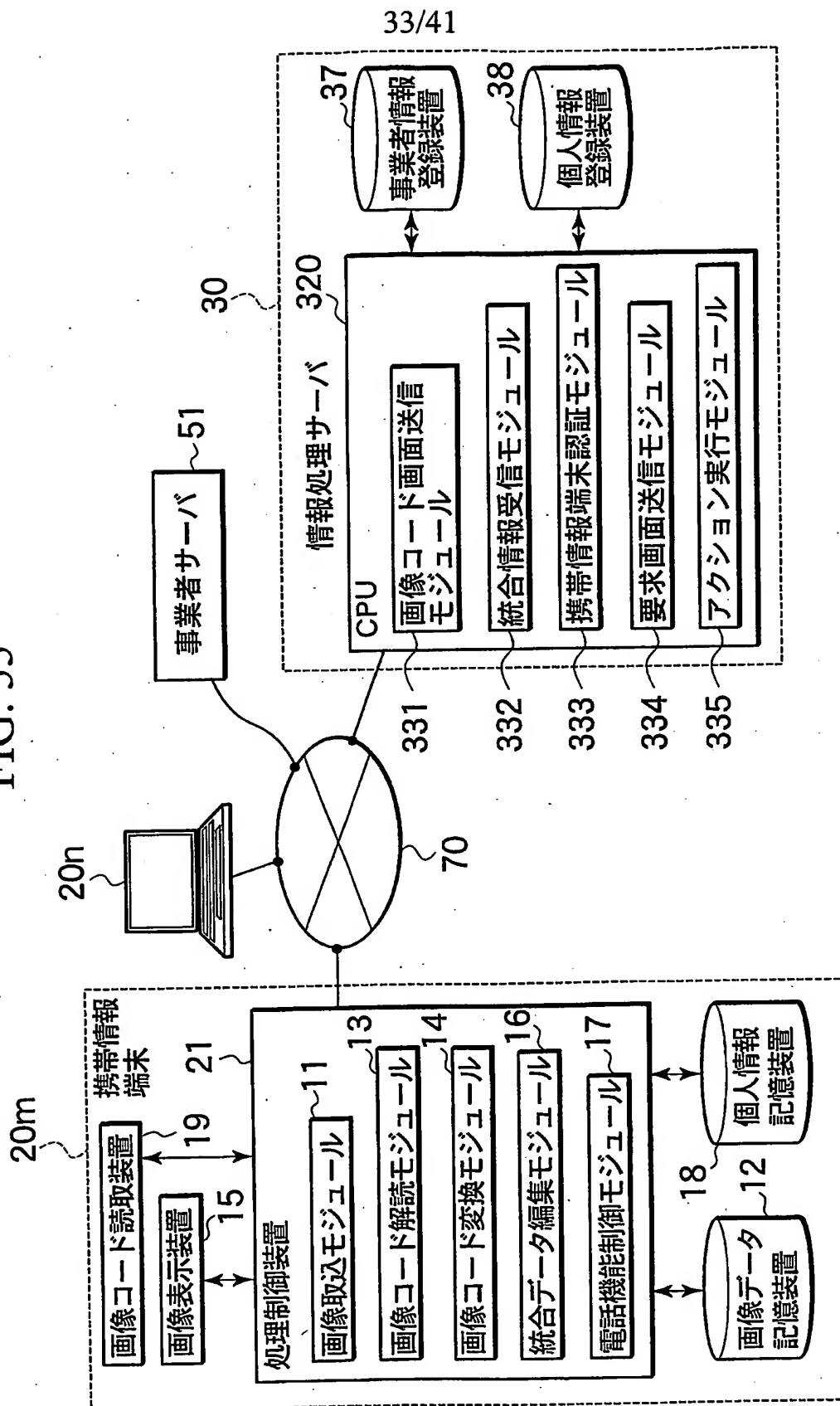




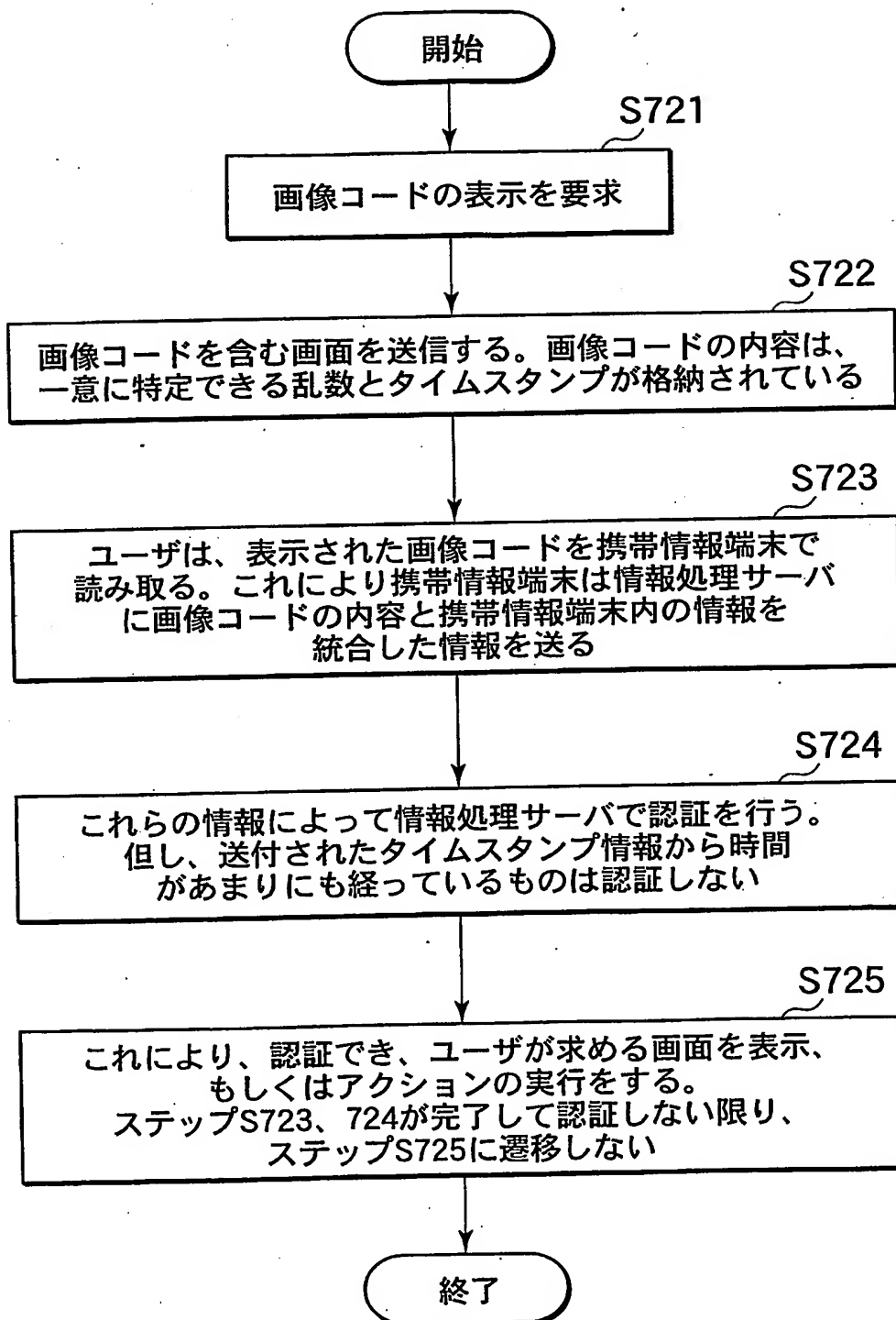


FIG. 33



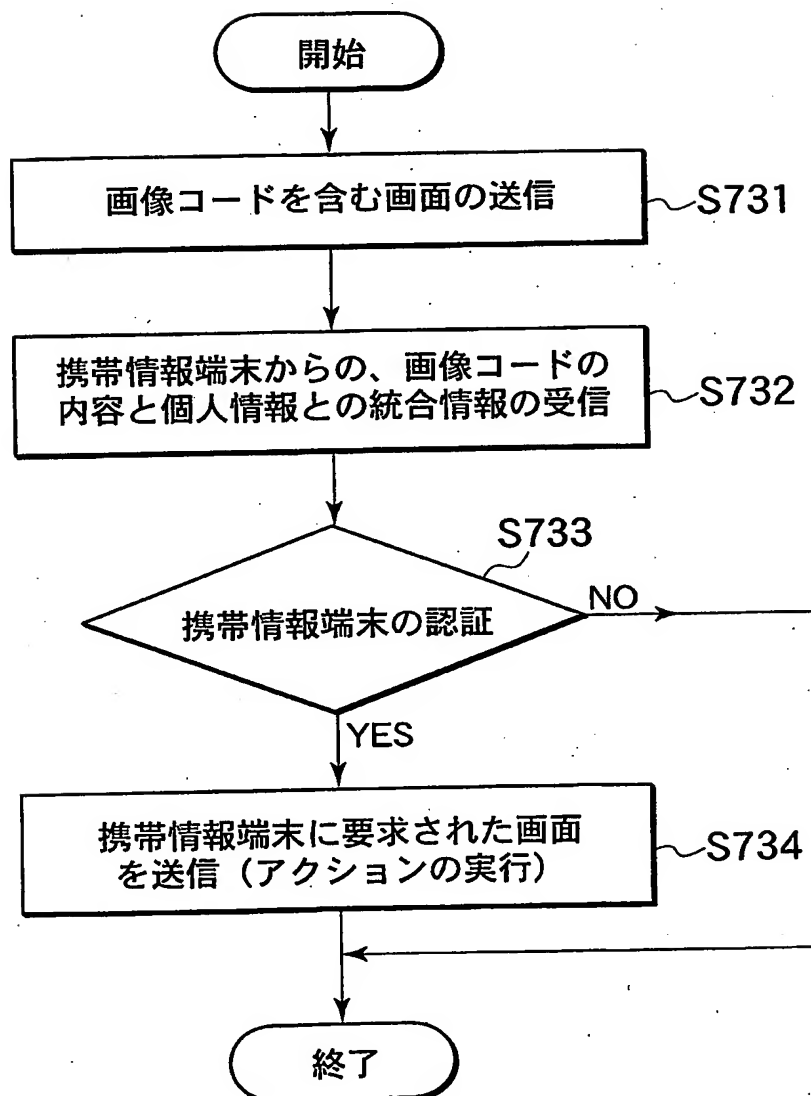
34/41

FIG. 34



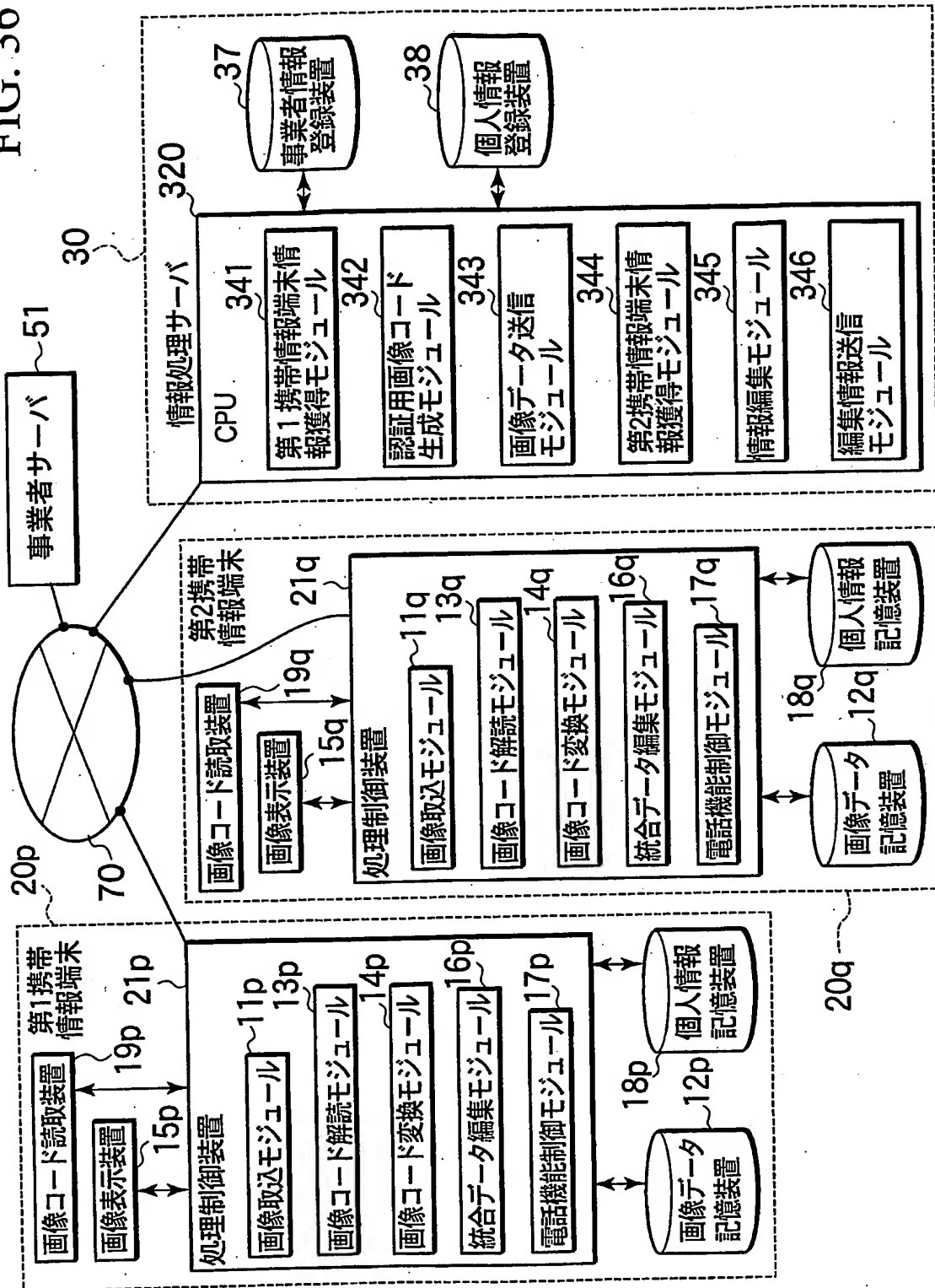
35/41

FIG. 35



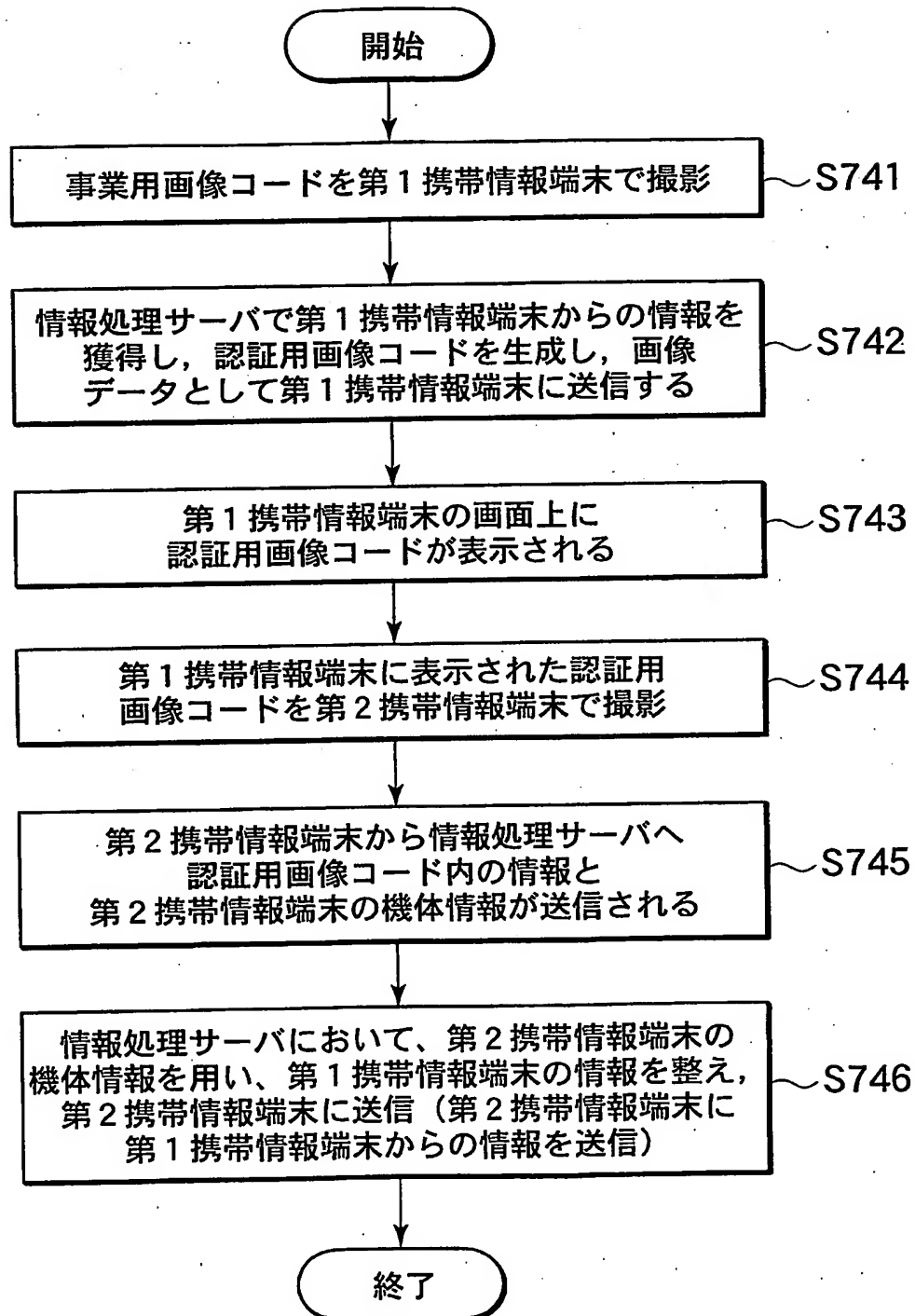
36/41

FIG. 36



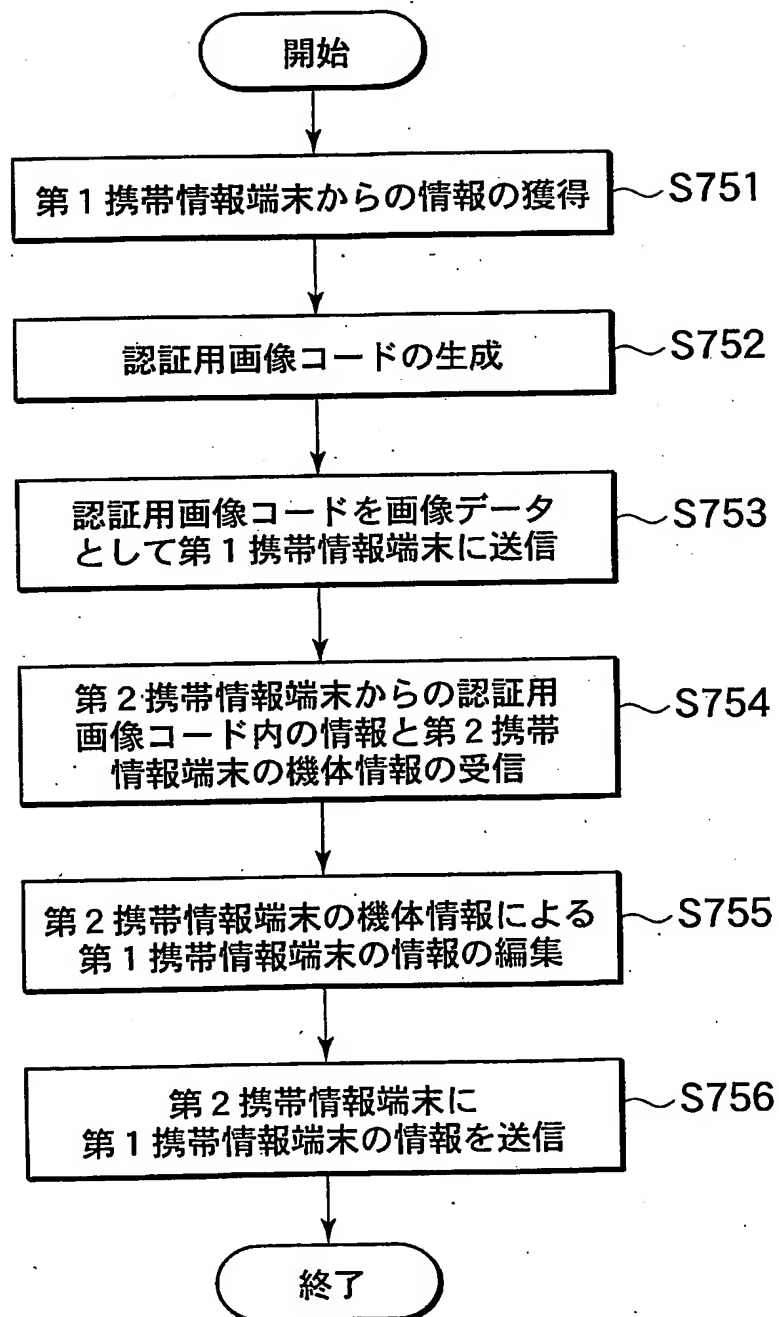
37/41

FIG. 37



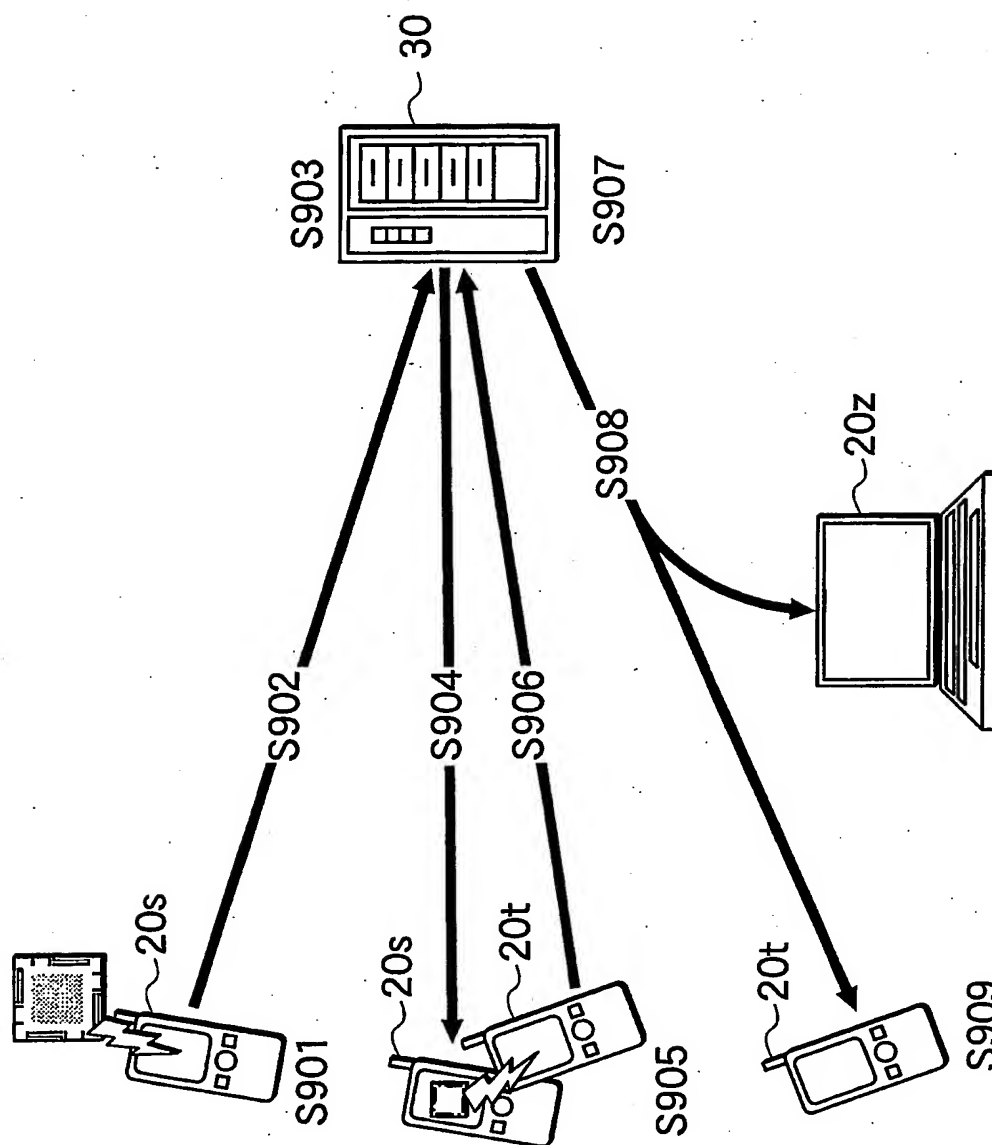
38/41

FIG. 38



39/41

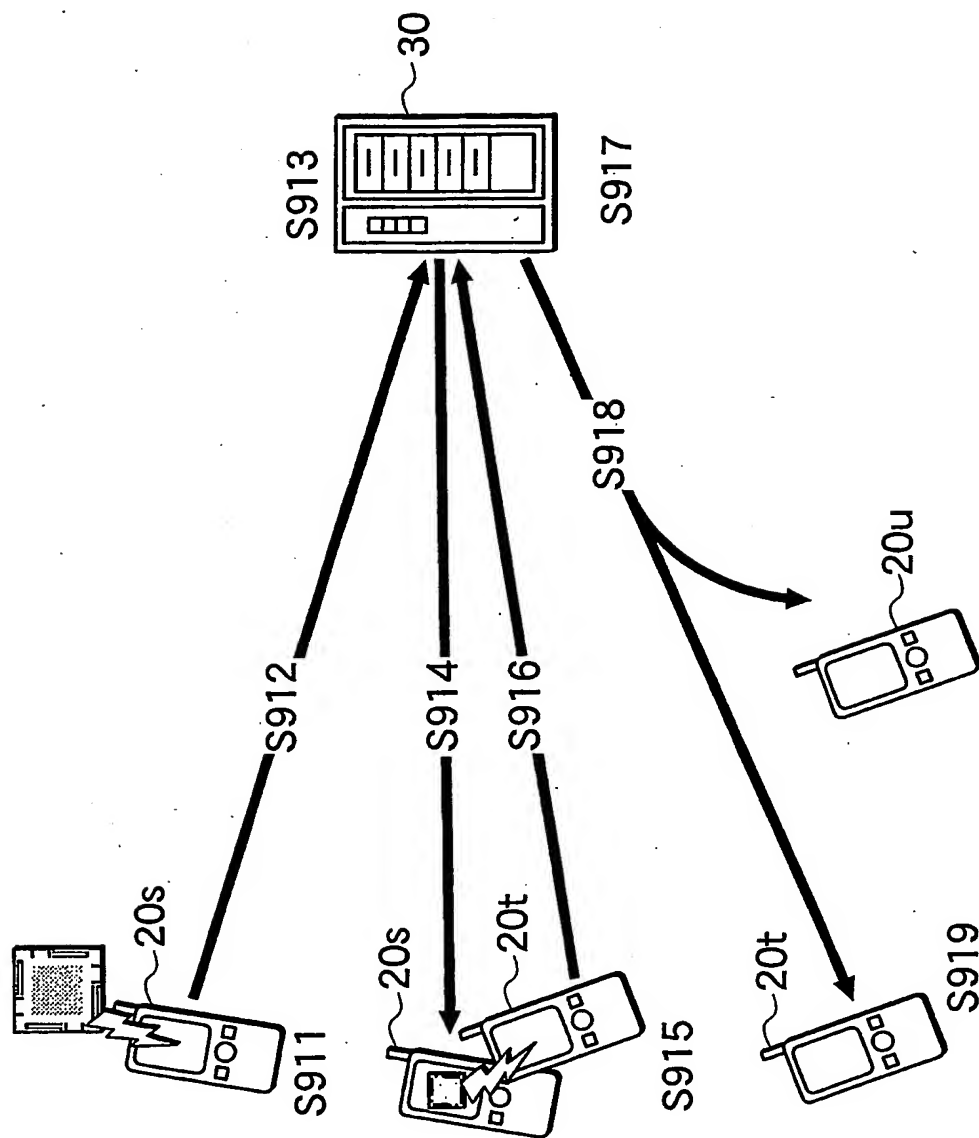
FIG. 39





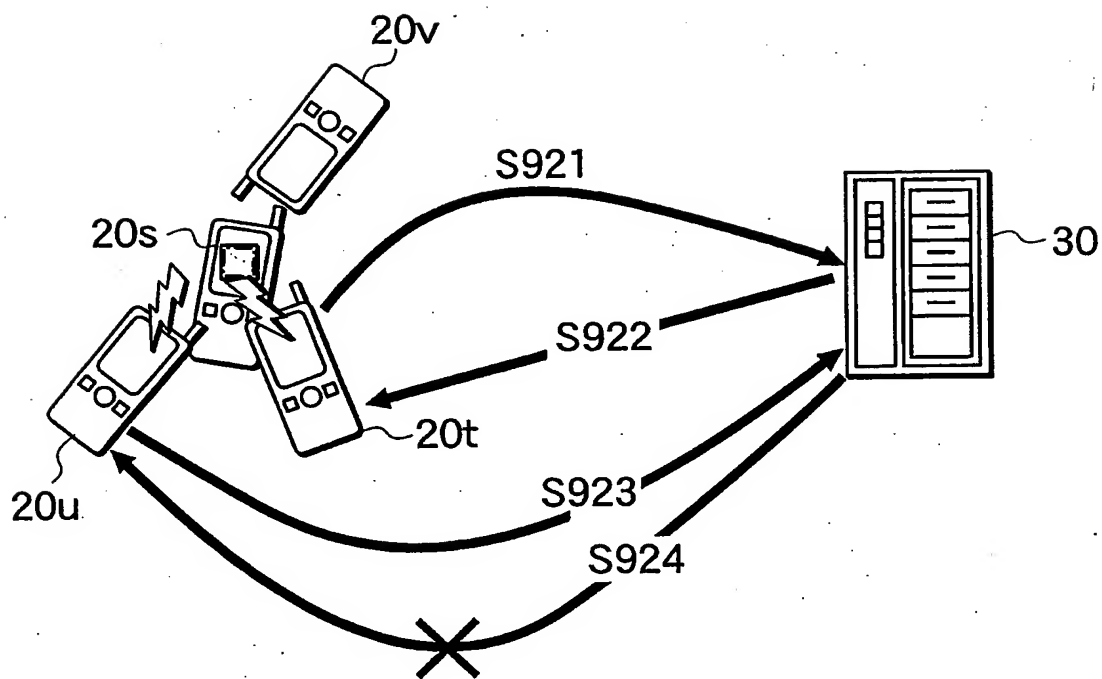
40/41

FIG. 40



41/41

FIG. 41



# INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007112

A. CLASSIFICATION OF SUBJECT MATTER  
Int.Cl<sup>7</sup> G06F15/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)  
Int.Cl<sup>7</sup> G06F15/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched  
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2004  
Kokai Jitsuyo Shinan Koho 1971-2004 Jitsuyo Shinan Toroku Koho 1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-344444 A (Sony Corp.), 29 November, 2002 (29.11.02), Full text; Figs. 1 to 27 & US 2002-184539 A	1-16
A	JP 2003-152713 A (Canon Inc.), 23 May, 2003 (23.05.03), Full text; Figs. 1 to 12 (Family: none)	1-16
X A	JP 2002-312280 A (Seiko Epson Corp.), 25 October, 2002 (25.10.02), Full text; Figs. 1 to 7 (Family: none)	17-19 20-23

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

\* Special categories of cited documents:  
"A" document defining the general state of the art which is not considered to be of particular relevance  
"E" earlier application or patent but published on or after the international filing date  
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)  
"O" document referring to an oral disclosure, use, exhibition or other means  
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention  
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone  
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art  
"&" document member of the same patent family

Date of the actual completion of the international search  
16 August, 2004 (16.08.04)

Date of mailing of the international search report  
31 August, 2004 (31.08.04)

Name and mailing address of the ISA/  
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

## INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP2004/007112

## C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2003-189020 A (Oto MATSUSHITA), 04 July, 2003 (04.07.03), Full text; Figs. 1 to 5 (Family: none)	17-23
A	JP 2001-222483 A (Sony Corp.), 17 August, 2001 (17.08.01), Full text; Figs. 1 to 14 (Family: none)	17-23

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2004/007112

**Box No. II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)**

This international search report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:  
because they relate to subject matter not required to be searched by this Authority, namely:
2. ☐ Claims Nos.:  
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:
3. ☐ Claims Nos.:  
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

**Box No. III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)**

This International Searching Authority found multiple inventions in this international application, as follows:

The inventions of claims 1-16 relate to a technical feature that a communication terminal having no authentication information is authenticated by judging whether authentication information in the authentication terminal coincides with the authentication information stored in the authentication information storage device and transmitting the result to the communication terminal.

(Continued to extra sheet.)

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:
4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

**Remark on Protest**

- ☐ The additional search fees were accompanied by the applicant's protest.  
☒ No protest accompanied the payment of additional search fees.

**INTERNATIONAL SEARCH REPORT**

International application No.

PCT/JP2004/007112

Continuation of Box No.III of continuation of first sheet(2)

The inventions of claims 17-23 relate to a technical feature that there are provided an identifier correspondence information storage device for storing correspondence information searched by a communication terminal identifier and an information conversion module for converting the information inputted from the communication terminal, according to the correspondence information.